

Contrail Service Orchestration Customer Portal User Guide

Published
2022-02-21

Release
6.1.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Contrail Service Orchestration Customer Portal User Guide

6.1.0

Copyright © 2022 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | xxx

Documentation and Release Notes | xxx

Documentation Conventions | xxx

Documentation Feedback | xxxiii

Requesting Technical Support | xxxiii

Self-Help Online Tools and Resources | xxxiv

Creating a Service Request with JTAC | xxxiv

1

Introduction

Customer Portal Overview | 2

About the Customer Portal User Guide | 2

Customer Portal Overview | 3

Accessing Customer Portal | 10

Personalize the Customer Portal | 12

Switching the Tenant Scope | 13

Setting Up Your Network with Customer Portal | 14

About the Customer Portal Dashboard | 15

Tasks You Can Perform | 15

Field Descriptions | 16

Changing the Customer Portal Password | 19

Resetting the Password | 19

Changing the Password on First Login | 21

Set a New Password After Your Existing Password Expires | 22

Configuring Two-Factor Authentication | 23

Extending the User Login Session | 25

Resend Activation Link in Customer Portal | 26

[View and Edit Tenant Settings | 27](#)

Users and Roles | 35

[Role-Based Access Control Overview | 35](#)

[About the Users Page in Customer Portal | 36](#)

[Tasks You Can Perform | 37](#)

[Field Descriptions | 37](#)

[Adding Tenant and OpCo Tenant Users | 38](#)

[Editing and Deleting Tenant and OpCo Tenant Users | 40](#)

[Editing Tenant and OpCo Tenant Users | 40](#)

[Deleting Tenant and OpCo Tenant Users | 41](#)

[Resetting the Password for Tenant Users | 41](#)

[Roles Overview | 42](#)

[Types of Roles | 42](#)

[Role Scopes | 43](#)

[Access Privileges | 43](#)

[Relationship Between User, Roles, and Access Privileges | 43](#)

[Benefits of role-based access control \(RBAC\) | 44](#)

[About the Tenant Roles Page | 45](#)

[Tasks You Can Perform | 45](#)

[Field Descriptions | 45](#)

[Adding User-Defined Roles for Tenant Users | 46](#)

[Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 47](#)

[Editing Roles | 48](#)

[Cloning Roles | 48](#)

[Deleting Roles | 49](#)

[Access Privileges for Role Scopes \(Tenant and Operating Company\) | 50](#)

SD-WAN and NGFW Deployments | 59

[SD-WAN and NGFW Workflows for a Tenant Administrator | 59](#)

[SD-WAN Deployment Workflow | 59](#)

[NFW Deployment Workflow | 62](#)

Managing Sites, Site Groups, and Site Templates

Managing Sites | 67

About the Site Management Page | 68

Tasks You Can Perform | 68

Field Descriptions | 69

Multihoming Overview | 71

Enterprise Hubs Overview | 71

Benefits of Enterprise Hubs | 72

Understand BGP Underlay Routing and Provider Edge (PE) Resiliency | 73

BGP Underlay Routing and Route Advertisements | 74

Benefits of BGP Underlay Routing and PE Resiliency | 74

Upgrading Sites Overview | 75

Add Enterprise Hubs with SD-WAN Capability | 76

Add Provider Hub Sites in SD-WAN Deployments | 103

Adding Cloud Spoke Sites for SD-WAN Deployment | 105

Provisioning a Cloud Spoke Site in AWS VPC | 115

Add a Cloud Spoke Site | 116

Download the Cloud Formation Template | 117

Provision the Device on AWS Server | 117

Activate the Device | 118

Manually Adding Branch Sites | 119

Add a Branch Site with SD-WAN Capability | 120

Adding and Provisioning a Next Generation Firewall Overview | 151

Overview | 151

Topology | 151

Workflow | 152

Enabling Integration with Mist Access Points | 152

Add a Standalone Next-Generation Firewall Site | 153

Managing LAN Segments on a Tenant Site | 161

Adding LAN Segments | 162

Edit a LAN segment | 168

Deploying LAN Segments | 169

Deleting LAN Segments | 170

Manage a Site	170
Start a Network Service	178
Disable a Network Service	180
Delete a Network Service	181
Add IP VPN Configuration to Provider Hubs	182
Edit IP VPN Configuration for Provider Hubs	185
Delete IP VPN Configuration from Provider Hubs	186
Viewing the Sites History	187
Viewing Jobs Initiated to Add and Configure Sites	187
Viewing Jobs Initiated to Delete Sites	188
Edit Site Overview	189
Benefits of Editing Site Parameters	192
Edit Branch and Enterprise Hub Site Parameters	192
Reconfigure Static Tunnels	203
Edit Site Examples	204
Example 1: Configure a Site with a LAN segment, WAN link, and Local Breakout Enabled	205
Example 2: Configure a Site with a LAN Segment, Active WAN Link, Backup WAN Link, and Local Breakout Enabled	206
Example 3: Configure a Site with a LAN Segment and Two Active WAN Links	207
Example 4: Configure a Site integrated with Zscaler	208
Example 5: Configure Site-to-Site Traffic Through DVPN Tunnels	209
Example 6: Configure a Fully Functional Site with Enterprise and Provider Hubs	210
Upgrading Sites	211
Upgrading Junos OS	211
Upgrading a Site	212
Upgrading Sites in Bulk	213
Delete a Site—Enterprise Hub, Cloud Spoke, and Branch	213
Managing Site Groups 	216
About the Site Groups Page	216
Tasks You Can Perform	216
Field Descriptions	217
Creating Site Groups	217

Managing Site Templates | 219

About the Site Templates Page | 219

Tasks You Can Perform | 219

Add Branch Sites by Using a Site Template | 220

Cloning, Editing, and Deleting Site Templates | 221

Cloning Site Templates | 222

Editing Site Templates | 222

Deleting Site Templates | 223

Adding a Site Template | 224

Adding and Configuring Sites by Importing a JSON File | 238

Managing Mesh Tags | 240

Mesh Tags Overview | 240

About the Mesh Tags Page | 241

Tasks You Can Perform | 241

Field Descriptions | 241

Creating User-defined Mesh Tags | 242

Managing Dynamic Mesh | 243

Dynamic Mesh Tunnels Overview | 243

Adding On-Demand Mesh Tunnels | 244

Deleting On-Demand Mesh Tunnels | 246

Managing Devices and Resources

Managing Devices | 249

Device Redundancy Support Overview | 250

Prerequisites for SRX Series Devices | 250

Supported Connection Plans | 250

Create and Configure an SD-WAN Site | 251

Dual CPE Devices Logical Topology for NFX Network Services Platform | 251

Dual CPE Devices Logical Topology for SRX Series Gateway Devices | 251

Activate a Device | 252

Manually Activate a Device That Supports Phone-Home Client | 253

Manually Activate a Device That Does Not Support Phone-Home Client | 254

Activating Dual CPE Devices (Device Redundancy) | 255

Viewing the History of Tenant Device Activation Logs | 257

Zero Touch Provisioning Overview | 259

Devices Supported | 260

Benefits | 261

Workflow for Onboarding a Device Using ZTP | 262

Configure an SRX Series CPE to Discover an EX Series Switch or AP Connected to the CPE | 265

Managing Device Images | 266

Device Images Overview | 266

About the Device Images Page | 266

Tasks You Can Perform | 266

Field Descriptions | 267

Deleting Device Images | 267

Managing Resources | 269

Multidepartment CPE Device Support | 270

- Overlapping IP Addresses Across Departments | 270**

About the Devices Page | 271

- Tasks You Can Perform | 272**

- Field Descriptions | 273**

Perform Return Material Authorization (RMA) for a Device | 275

- Perform Return Material Authorization (RMA) for a Single-CPE, Enterprise Hub and Next-Generation Firewall | 276**

- Perform Return Material Authorization (RMA) for a Dual-CPE Device | 278**

- Perform RMA for an NFX Cluster | 278**

- Perform RMA for an SRX Cluster | 281**

Grant Return Material Authorization (RMA) for a Device | 283

- Grant Return Material Authorization (RMA) for a Single-CPE, Enterprise Hub, and Next-Generation Firewall | 283**

- Grant RMA for a Dual-CPE Device | 285**

- Grant RMA for an SRX Device within an SRX Cluster | 287**

Manage a Single CPE Device | 288

Rebooting a CPE Device | 290

Configuring APN Settings on CPE Devices | 291

- Configuring APN Settings with SIM Change on CPE Devices | 291**

- Configuring APN Settings without SIM Change on CPE Devices | 293**

Identifying Connectivity Issues by Using Ping | 294

Identifying Connectivity Issues by Using Traceroute | 298

Remotely Accessing a Device CLI | 300

View the Current Configuration on a Device | 301

Generate Device RSI for Enterprise Hub and Spoke Devices | 302

Configuring the Firewall Device | 303

About the Physical Interfaces Page | 305

- Tasks You Can Perform | 305**

- Field Descriptions | 306**

About the Logical Interfaces Page | 306

- Tasks You Can Perform | 306**

- Field Descriptions | 307**

[Adding a Logical Interface | 307](#)

[Editing, Deleting, and Deploying Logical Interfaces | 310](#)

[Editing Logical Interfaces | 310](#)

[Deleting Logical Interfaces | 311](#)

[Deploying Logical Interfaces | 311](#)

[Enable LLDP on a CPE Interface | 311](#)

[Create LAG Interface | 312](#)

[Create a RETH Interface | 314](#)

[Create a Redundancy Group | 316](#)

[Manage Redundancy Groups | 317](#)

[Adding a Security Zone | 318](#)

[Adding a Routing Instance | 321](#)

[Create Management Connectivity Between a CPE and a Switch | 322](#)

[Discover an EX Series Switch or APs Configured Behind a CPE | 325](#)

[View an EX Series Switch or an AP on Mist | 325](#)

[View an SRX Series CPE on Juniper Mist | 326](#)

[About the Static Routes Page | 326](#)

[Tasks You Can Perform | 326](#)

[Field Descriptions | 327](#)

[Adding a Static Route | 327](#)

[Editing, Deleting, and Deploying Static Routes | 330](#)

[Editing Static Routes | 330](#)

[Deleting Static Routes | 331](#)

[Deploying Static Routes | 331](#)

[Managing Device Templates | 332](#)

[Device Template Overview | 332](#)

[Platform | 333](#)

[SD-WAN CPE | 333](#)

[Secure Internet CPE | 335](#)

[Managed Internet CPE | 336](#)

[About the Device Template Page | 337](#)

[Tasks You Can Perform | 337](#)

[Field Descriptions | 337](#)

Supported Device Templates	338
Cloning a Device Template	340
Importing a Device Template	341
Creating a Device Template File	342
Importing a Device Template File	342
Updating Stage-2 Configuration Template in a Device Template	343
Configuring Stage-2 Initial Configuration in a Device Template	348
Managing Configuration Templates 	351
Configuration Templates Overview	351
Benefits	352
Configuration Templates Workflow	353
About the Configuration Templates Page	354
Tasks You Can Perform	354
Field Descriptions	355
Predefined Configuration Templates	357
Edit, Clone, and Delete Configuration Templates	361
Edit a Configuration Template	361
Clone a Configuration Template	362
Delete a Configuration Template	363
Deploy Configuration Templates to Devices	363
Deploy from the Configuration Templates Page	364
Deploy from the Devices Page	368
Undeploy a Configuration Template from a Device	369
Dissociate a Configuration Template from a Device	371
Preview and Render Configuration Templates	371
Import Configuration Templates	373
Export a Configuration Template	375
Assign Configuration Templates to Device Templates	376
Add Configuration Templates	378
Jinja Syntax and Examples for Configuration Templates	387
Jinja Syntax and CSO Keywords	388
Example 1: Convert a Single Junos OS Command to Jinja Syntax	390
Example 2: Convert a Junos OS Configuration Snippet to Jinja Syntax	391

- Example 3: Use Conditional Logic | 393
- Example 4: Use Variable Substitution | 395
- Example 5: Use Filters, Concatenation, and Set Variables | 396
- Example 6: Test a Value | 397

View the Configuration Deployed on Devices | 399

Managing Licenses | 401

About the Device Licenses Page | 401

- Tasks You Can Perform | 401
- Field Descriptions | 402

Add a Device License File | 403

Edit a Device License File | 404

Delete a Device License File | 404

Push a Device License File | 405

About the CSO Licenses Page | 406

- Tasks You Can Perform | 406
- Field Descriptions | 407

Managing Signature Database and Certificates | 409

Signature Database Overview | 409

About the Signature Database Page | 410

- Tasks You Can Perform | 410
- Field Descriptions | 410

Manually Installing Signatures | 411

Automating Signature Database Installation | 413

Managing Signature Installation Settings (Auto Installation) | 416

Certificates Overview | 416

About the Certificates Page | 417

- Tasks You Can Perform | 417
- Field Descriptions | 417

Importing a Certificate | 419

Installing and Uninstalling Certificates | 421

- Installing a Certificate | 421
- Uninstalling a Certificate | 422

About the VPN Authentication Page | 422

Tasks You Can Perform | 423

Field Descriptions | 423

Modify PKI Settings for All Sites | 425

Modify PKI Settings for Selected Sites | 428

Managing Juniper Identity Management Service | 430

Juniper Identity Management Service Overview | 430

Access Token Query | 431

Batch or Periodic Query | 431

IP Address Query | 432

User Mapping Query | 432

About the Identity Management Page | 433

Tasks You Can Perform | 433

Configuring CSO and JIMS Connection | 434

Configuring JIMS for an SRX Device | 436

4

Managing Policies, Profiles, and Proxies

Managing Firewall Policies | 440

Firewall Policy Overview | 441

About the Firewall Policy List Page | 443

Tasks You Can Perform | 443

Field Descriptions | 443

About the Firewall Policy Name Page | 444

Tasks You Can Perform | 444

Field Descriptions | 445

Adding a Firewall Policy | 445

Editing and Deleting Firewall Policies | 447

Editing Firewall Policies | 448

Deleting Firewall Policies | 448

Adding Firewall Policy Intents | 449

Editing, Cloning, and Deleting Firewall Policy Intents | 455

Editing Firewall Policy Intents | 456

Cloning Firewall Policy Intents | 456

Deleting Firewall Policy Intents | 457

Selecting Firewall Source | 457

Adding an End Point as Firewall Source | 458

Selecting Firewall Source Using Abbreviations | 459

Selecting a Firewall Source from the End Points Panel | 459

Creating and Selecting a Firewall Source from the End Points Panel | 460

Creating Addresses from Source | 460

Selecting Firewall Destination | 461

Adding an End Point as Firewall Destination | 461

Selecting Firewall Destination Using Abbreviations | 462

Selecting a Firewall Destination from the End Points Panel | 462

Creating and Selecting a Firewall Destination from the End Points Panel | 463

Creating Addresses from Destination | 463

Firewall Policy Examples | 464

Example 1: Firewall Policy that Permits Traffic from Departments in Site A to the Departments in Site B | 466

Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B | 468

Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B | 471

Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A | 472

Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments | 474

Example 6: Firewall Policy that Denies Access to Social Networking Sites | 482

Example 7: Firewall Policy that Controls Access to an Address over the Internet (HTTP) | 485

Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service | 491

Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B | 493

Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A | 496

Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled | 500

Example 12: Firewall Policy that blocks access to Internet and allow access to Google Drive. | 503

Firewall Policy Schedules Overview | 504

About the Firewall Policy Schedules Page | 505

Tasks You Can Perform | 505

Field Descriptions | 505

Creating Schedules | 506

Editing, Cloning, and Deleting Schedules | 508

Editing Schedules | 508

Cloning Schedules | 508

Deleting Schedules | 509

Deploying Firewall Policies | 509

About the Default Profiles for Unified Firewall Policy Page | 510

Tasks You Can Perform | 511

Field Descriptions | 511

Editing Default Settings for the Unified Firewall Policy | 512

Importing Policies Overview | 514

Importing Firewall Policies | 516

Managing UTM Profiles | 518

UTM Overview | 519

UTM Licensing | 520

UTM Components | 520

Configuring UTM Settings | 521

About the UTM Profiles Page | 523

Tasks You Can Perform | 523

Field Descriptions | 523

Creating UTM Profiles | 525

Editing, Cloning, and Deleting UTM Profiles | 528

Editing UTM Profiles | 528

Cloning UTM Profiles | 529

Deleting UTM Profiles | 529

About the Web Filtering Profiles Page	530
Tasks You Can Perform	530
Field Descriptions	531
Creating Web Filtering Profiles	532
Editing, Cloning, and Deleting Web Filtering Profiles	536
Editing Web Filtering Profiles	537
Cloning Web Filtering Profiles	537
Deleting Web Filtering Profiles	538
About the Antivirus Profiles Page	538
Tasks You Can Perform	539
Field Descriptions	539
Creating Antivirus Profiles	540
Editing, Cloning, and Deleting Antivirus Profiles	543
Editing Antivirus Profiles	543
Cloning Antivirus Profiles	543
Deleting Antivirus Profiles	544
About the Antispam Profiles Page	545
Tasks You Can Perform	545
Field Descriptions	545
Creating Antispam Profiles	546
Editing, Cloning, and Deleting Antispam Profiles	548
Editing Antispam Profiles	549
Cloning Antispam Profiles	549
Deleting Antispam Profiles	550
About the Content Filtering Profiles Page	550
Tasks You Can Perform	550
Field Descriptions	551
Creating Content Filtering Profiles	552
Editing, Cloning, and Deleting Content Filtering Profiles	556
Editing Content Filtering Profiles	556
Cloning Content Filtering Profiles	556
Deleting Content Filtering Profiles	557

About the URL Patterns Page | 558**Tasks You Can Perform | 558****Field Descriptions | 558****Creating URL Patterns | 559****Editing, Cloning, and Deleting URL Patterns | 560****Editing URL Patterns | 561****Cloning URL Patterns | 561****Deleting URL Patterns | 562****About the URL Categories Page | 562****Tasks You Can Perform | 562****Field Descriptions | 563****Creating URL Categories | 563****Editing, Cloning, and Deleting URL Categories | 565****Editing URL Categories | 565****Cloning URL Categories | 565****Deleting URL Categories | 566****Managing SLA Profiles and SD-WAN Policies | 567****Traffic Steering Profiles and SD-WAN Policies Overview | 568****Traffic Steering Profiles | 568****SD-WAN Policies | 571****About the SD-WAN Policy Page | 573****Tasks You Can Perform | 573****Field Descriptions | 574****Creating SD-WAN Policy Intents | 575****Editing and Deleting SD-WAN Policy Intents | 583****Editing SD-WAN Policy Intents | 583****Deleting SD-WAN Policy Intents | 584****Application Quality of Experience Overview | 584****Benefits of Application Quality of Experience | 586****Configure and Monitor Application Quality of Experience | 586**

About the SLA-Based Steering Profiles Page	587
Tasks You Can Perform	587
Field Descriptions	588
Adding SLA-Based Steering Profiles	591
Editing and Deleting SLA-Based Steering Profiles	598
Editing an SLA-Based Steering Profile	598
Deleting SLA-Based Steering Profiles	599
About the Path-Based Steering Profiles Page	600
Tasks You Can Perform	600
Field Descriptions	600
Adding Path-Based Steering Profiles	602
Editing and Deleting Path-Based Steering Profiles	604
Editing a Path-Based Steering Profile	605
Deleting a Path-Based Steering Profile	606
Breakout and Breakout Profiles Overview	606
Cloud Breakout	608
Breakout Profiles	608
SD-WAN Policy Intents for Breakout	608
Benefits of Breakout Profiles	609
About the Breakout Profiles Page	609
Tasks You Can Perform	610
Breakout Profiles Field Descriptions	610
Cloud Breakout Settings Field Descriptions	612
Adding Breakout Profiles	614
Adding Cloud Breakout Settings	616
Assigning Cloud Breakout Settings to Sites	620
Detaching Cloud Breakout Settings from Sites	622
Editing Breakout Profiles and Cloud Breakout Settings	623
Editing Breakout Profiles	623
Editing Cloud Breakout Settings	624
Deleting Breakout Profiles and Cloud Breakout Settings	625
Deleting Breakout Profiles	625
Deleting Cloud Breakout Settings	625
Configuring Breakout on SD-WAN Sites	626

Managing NAT Policies | 628

NAT Policies Overview | 629

About the NAT Policies Page | 632

Tasks You Can Perform | 632

Field Descriptions | 632

Creating NAT Policies | 633

Editing and Deleting NAT Policies | 635

Editing NAT Policies | 635

Deleting NAT Policies | 635

About the Single NAT Policy Page | 636

Tasks You Can Perform | 636

Field Descriptions | 637

Creating NAT Policy Rules | 638

Editing, Cloning, and Deleting NAT Policy Rules | 645

Editing NAT Policy Rules | 645

Cloning NAT Policy Rules | 645

Deleting NAT Policy Rules | 646

Deploying NAT Policy Rules | 647

Selecting NAT Source | 648

Adding an Endpoint as NAT Source | 648

Selecting Interfaces when GWR Resides Inside an NFX Box | 648

Selecting NAT Source Using Abbreviations | 649

Selecting a NAT Source from the End Points Panel | 650

Creating and Selecting a NAT Source from the End Points Panel | 650

Creating Addresses from Source Field | 651

Selecting NAT Destination | 652

Adding an Endpoint as NAT Destination | 652

Selecting Interfaces when GWR Resides Inside an NFX Box | 652

Selecting NAT Destination Using Abbreviations | 653

Selecting a NAT Destination from the End Points Panel | 654

Creating and Selecting a NAT Destination from the End Points Panel | 654

Creating Addresses from Destination Field | 655

Creating Services from Destination Field | 655

NAT Pools Overview | 656

About the NAT Pools Page | 656

Tasks You Can Perform | 657

Creating NAT Pools | 658

Editing, Cloning, and Deleting NAT Pools | 660

Editing NAT Pools | 660

Cloning NAT Pools | 661

Deleting NAT Pools | 661

Deploying NAT Policies | 662

Importing NAT Policies | 662

Managing IPS Signatures and Profiles | 665

About the IPS Signatures Page | 665

Tasks You Can Perform | 666

Field Descriptions | 666

Create IPS Signatures | 670

Create IPS Signature Static Groups | 678

Create IPS Signature Dynamic Groups | 679

Edit, Clone, and Delete IPS Signatures | 685

Edit IPS Signatures | 685

Clone IPS Signatures | 686

Delete IPS Signatures | 686

Edit, Clone, and Delete IPS Signature Static Groups | 687

Edit IPS Signature Static Groups | 687

Clone IPS Signature Static Groups | 688

Delete IPS Signature Static Groups | 689

Edit, Clone, and Delete IPS Signature Dynamic Groups | 690

Edit IPS Signature Dynamic Groups | 690

Clone IPS Signature Dynamic Groups | 691

Delete IPS Signature Dynamic Groups | 692

About the IPS Profiles Page | 692

Tasks You Can Perform | 693

Field Descriptions | 693

Create IPS Profiles | 694

Edit, Clone, and Delete IPS Profiles | 695**Edit IPS Profiles | 695****Clone IPS Profiles | 696****Delete IPS Profiles | 696****About the <IPS-Profile-Name> / Rules Page | 697****Tasks You Can Perform | 697****Field Descriptions | 698****Create IPS or Exempt Rules | 699****Create IPS Rules | 699****Create Exempt Rules | 706****Edit, Clone, and Delete IPS or Exempt Rules | 707****Edit IPS or Exempt Rules | 707****Clone IPS or Exempt Rules | 708****Delete IPS or Exempt Rules | 708****Managing SSL Proxies | 710****SSL Forward Proxy Overview | 710****Supported Ciphers in Proxy Mode | 712****Server Authentication | 713****Root CA | 714****Trusted CA List | 714****Session Resumption | 715****SSL Proxy Logs | 715****About the SSL Proxy Policy Page | 716****Tasks You Can Perform | 717****Field Descriptions | 717****Creating SSL Proxy Policy Intents | 718****Editing, Cloning, and Deleting SSL Proxy Policy Intents | 722****Editing SSL Proxy Policy Intents | 723****Cloning SSL Proxy Policy Intents | 723****Deleting SSL Proxy Policy Intents | 724****Understanding How SSL Proxy Policy Intents Are Applied | 725****Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match | 725****Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match | 726**

Example 3: Applying SSL Proxy Policy Intents on Internal (Site-to-Site) Traffic | 726

About the SSL Proxy Profiles Page | 727

Tasks You Can Perform | 727

Widget Descriptions | 728

Creating SSL Forward Proxy Profiles | 729

Editing, Cloning, and Deleting SSL Forward Proxy Profiles | 733

Editing SSL Forward Proxy Profiles | 734

Cloning SSL Forward Proxy Profiles | 734

Deleting SSL Forward Proxy Profiles | 735

Configuring and Deploying an SSL Forward Proxy Policy | 736

Deploying Policies | 738

Deploying Policies Overview | 738

About the Deployments Page | 739

Tasks You Can Perform | 739

Field Descriptions | 739

Using the Deployment Icon to Deploy Policies | 741

Deploying Policies | 742

5

Managing Network Services and Shared Objects

Configuring Network Services | 745

Network Service Overview | 745

About the Network Services Page | 746

Tasks You Can Perform | 746

Field Descriptions | 746

About the Service Instances Page | 748

Tasks You Can Perform | 748

Field Descriptions | 748

Managing Shared Objects | 750

Addresses and Address Groups Overview | 751

About the Addresses Page | 751

Tasks You Can Perform | 751

Field Descriptions | 752

Creating Addresses or Address Groups | 753

Editing, Cloning, and Deleting Addresses and Address Groups | 755

Editing Addresses and Address Groups | 756

Cloning Addresses and Address Groups | 756

Deleting Addresses and Address Groups | 757

Services and Service Groups Overview | 758

About the Services Page | 758

Tasks You Can Perform | 758

Field Descriptions | 759

Creating Services and Service Groups | 759

Creating Protocols | 761

Editing and Deleting Protocols | 765

Editing Protocols | 765

Deleting Protocols | 766

Editing, Cloning, and Deleting Services and Service Groups | 766

Editing Services and Service Groups | 767

Cloning Services or Service Groups | 767

Deleting Services and Service Groups | 768

Application Signatures Overview | 768

About the Application Signatures Page | 769

Tasks You Can Perform | 769

Field Descriptions | 769

Understanding Custom Application Signatures | 770

Adding Application Signatures | 772

Editing, Cloning, and Deleting Application Signatures | 777

- Editing Application Signatures | 777

- Cloning Application Signatures | 778

- Deleting Application Signatures | 778

Adding Application Signature Groups | 779

Editing, Cloning, and Deleting Application Signature Groups | 780

- Editing Application Signature Groups | 780

- Cloning Application Signature Groups | 780

- Deleting Application Signature Groups | 781

About the Departments Page | 781

- Tasks You Can Perform | 782

- Field Descriptions | 783

Add a Department | 783

Delete a Department | 785

About the Protocols Page | 785

- Tasks You Can Perform | 786

- Field Descriptions | 786

Add a Protocol Endpoint | 786

Edit or Delete Protocol Endpoint | 787

- Edit Protocols | 788

- Delete Protocols | 788

6

Monitoring Jobs and Audit Logs

Managing Jobs | 791

About the Jobs Page | 791

- Tasks You Can Perform | 791

- Field Descriptions | 791

Field Descriptions | 792

Editing and Deleting Scheduled Jobs | 793

Editing Scheduled Jobs | 794

Deleting Scheduled Jobs | 794

Viewing Job Details | 795

Retrying a Failed Job on Devices | 796

Managing Audit Logs | 797

Audit Logs Overview | 797

About the Audit Logs Page | 798

Tasks You Can Perform | 798

Viewing the Details of an Audit Log | 799

Exporting Audit Logs | 802

Purging Audit Logs (After Archiving or Without Archiving) | 803

Monitoring Alarms, Events, and Threats

Monitoring Security Alerts and Alarms | 808

About the Monitor Overview Page | 808

Tasks You Can Perform | 808

Field Descriptions | 809

Alerts Overview | 810

About the Generated Alerts Page | 810

Tasks You Can Perform | 811

Field Descriptions | 811

About the Alert Definitions/Notifications Page | 812

Tasks You Can Perform | 812

Managing Security Alerts Definitions | 813

Tasks You Can Perform | 813

Field Descriptions | 813

Creating Security Alert Definitions | 814

Editing, Cloning, and Deleting Security Alert Definitions | 815

Editing Security Alert Definitions | 816

Cloning Security Alert Definitions | 816

Deleting Security Alert Definitions | 816

About the Alarms Page | 817**Tasks You Can Perform | 818****Field Descriptions | 818****Enable E-mail Notifications for SD-WAN Alarms | 819****Rogue Device Detection | 821****Monitoring Security | 823****About the All Security Events Page | 823****Tasks You Can Perform | 823****Summary View | 824****Detail View | 824****About the Firewall Events Page | 828****Tasks You Can Perform | 828****Summary View | 828****Detail View | 829****About the Web Filtering Events Page | 831****Tasks You Can Perform | 831****Summary View | 831****Detail View | 832****About the IPsec VPNs Events Page | 834****Tasks You Can Perform | 834****Summary View | 834****Detail View | 835****About the Content Filtering Events Page | 836****Tasks You Can Perform | 836****Summary View | 836****Detail View | 837****About the Antispam Events Page | 838****Tasks You Can Perform | 838****Summary View | 839****Detail View | 839****About the Antivirus Events Page | 840****Tasks You Can Perform | 840****Summary View | 841**

Detail View | 841

About the IPS Events Page | 843

Tasks You Can Perform | 843

Summary View | 843

Detail View | 844

About the Screen Events Page | 846

Tasks You Can Perform | 846

Summary View | 847

Detail View | 847

About the Traffic Logs Page | 850

Tasks You Can Perform | 850

Monitoring SD-WAN Events | 853

SD-WAN Events Overview | 853

About the SD-WAN Events Page | 854

Tasks You Can Perform | 854

Field Descriptions | 854

Monitoring Applications | 856

About the SLA Performance of a Single Tenant Page | 856

Tasks You Can Perform | 856

Field Descriptions | 857

Viewing the SLA Performance of a Site | 859

SLA Not Met by SLA Profiles | 859

Applications SLA Performance by Throughput | 860

SLA Performance for ALL | 862

Viewing the SLA Performance of an Application or Application Group | 863

Application Visibility Overview | 865

Benefits of Application Visibility | 865

About the Application Visibility Page | 866

Tasks You Can Perform | 866

Chart View | 866

Grid View | 867

About the User Visibility Page | 869

Tasks You Can Perform | 869

Chart View | 869

Grid View | 871

Viewing Application or User Visibility Data for Specific Sites | 872

Viewing Application Visibility Data for Specific Sites | 872

Viewing User Visibility Data for Specific Sites | 873

Monitoring Threats | 875

About the Threats Map (Live) Page | 875

Tasks You Can Perform | 876

Field Descriptions | 877

Threat Types | 878

Managing Reports

Security Reports | 882

Reports Overview | 882

About the Security Report Definitions Page | 883

Tasks You Can Perform | 884

Field Descriptions | 884

Scheduling, Generating, Previewing, and Sharing Security Reports | 886

Editing Report Generation Schedule | 886

Generating Reports | 887

Previewing Reports in PDF | 888

Sharing Reports through E-mail | 888

About the Security Generated Reports Page | 889

Field Descriptions | 889

Creating Log Report Definition | 890

Creating Bandwidth Report Definition | 894

Creating ANR Report Definition | 896

Editing, Deleting, and Cloning Log Report Definitions | 899

Editing the Log Report Definition | 899

Deleting Log Report Definitions | 899

Cloning Log Report Definitions | 900

Editing, Deleting, and Cloning Bandwidth Report Definitions | 901**Editing Bandwidth Report Definitions | 901****Deleting Bandwidth Report Definitions | 901****Cloning Bandwidth Report Definitions | 902****Editing, Deleting, and Cloning ANR Report Definitions | 903****Editing ANR Report Definitions | 903****Deleting ANR Report Definitions | 904****Cloning ANR Report Definitions | 904****SD-WAN Reports | 906****About the SD-WAN Report Definitions Page | 906****Tasks You Can Perform | 906****Field Descriptions | 907****Editing, Deleting, and Cloning SD-WAN Report Definitions | 908****Editing the SD-WAN Report Definition | 908****Deleting SD-WAN Report Definitions | 908****Cloning SD-WAN Report Definitions | 909****Creating SD-WAN Tenant Performance Report Definitions | 910****Creating SD-WAN Site Performance Report Definitions | 914****About the SD-WAN Generated Reports Page | 917****Field Descriptions | 917**

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xxx
- Documentation Conventions | xxx
- Documentation Feedback | xxxiii
- Requesting Technical Support | xxxiii

Use this guide to understand the features and tasks that you can configure and perform from the Cloud-based Contrail Service Orchestration (CSO) Customer Portal UI . This guide provides, feature overviews, and procedures that help you understand the features and perform CSO configuration tasks.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page xxxi defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xxxi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

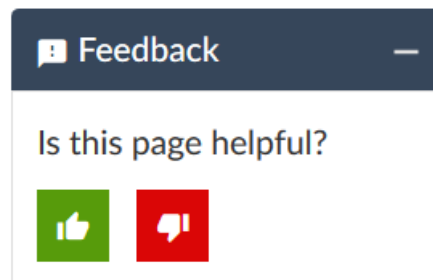
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

PART

Introduction

Customer Portal Overview | 2

Users and Roles | 35

SD-WAN and NGFW Deployments | 59

Customer Portal Overview

IN THIS CHAPTER

- About the Customer Portal User Guide | 2
- Customer Portal Overview | 3
- Accessing Customer Portal | 10
- Personalize the Customer Portal | 12
- Switching the Tenant Scope | 13
- Setting Up Your Network with Customer Portal | 14
- About the Customer Portal Dashboard | 15
- Changing the Customer Portal Password | 19
- Resetting the Password | 19
- Changing the Password on First Login | 21
- Set a New Password After Your Existing Password Expires | 22
- Configuring Two-Factor Authentication | 23
- Extending the User Login Session | 25
- Resend Activation Link in Customer Portal | 26
- View and Edit Tenant Settings | 27

About the Customer Portal User Guide

This guide provides an understanding of how to use the Contrail Service Orchestration (CSO) Customer Portal to implement your use cases. This guide is appropriate for tenant administrators and operators who need to know how to use Customer Portal.

Refer to [Table 3 on page 3](#) for additional CSO documentation resources.

Table 3: Additional CSO Documentation Resources

Title	Available At
What is SD-WAN?	https://www.juniper.net/us/en/products-services/what-is/sd-wan/
What is Network Functions Virtualization (NFV)?	https://www.juniper.net/us/en/products-services/what-is/network-functions-virtualization/
Learn About NFV	https://www.juniper.net/documentation/en_US/learn-about/LearnAbout_NFV.pdf
Administration Portal User Guide	https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration (User Guides section)
Other Resources	https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration

RELATED DOCUMENTATION

| [Customer Portal Overview](#) | 3

Customer Portal Overview

The Customer Portal in Contrail Service Orchestration (CSO) provides a Web-based UI that tenants of service providers (SPs) and operating companies (OpCos) can use to manage sites and devices, apply policies (firewall, NAT, SD-WAN, and so on), and perform administrative tasks. In Customer Portal, the objects that you manage and the actions that you perform are done in the context of a single tenant. Therefore, objects belonging to one tenant are isolated from objects belonging to other tenants.

Customer Portal supports role-based access control (RBAC), which means that the roles assigned to users determine their access privileges and the actions that they can perform. The following predefined roles are available in Customer Portal:

- Tenant Admin
- Tenant Operator

Administrator users have read access and write access to the Customer Portal UI and API capabilities, whereas operator users only have read access. Administrators can also create more users with specific roles and access privileges.

When you log in to Customer Portal, the main menu (left sidebar) that is displayed and the actions that you can perform depend on your access privileges. [Table 4 on page 4](#) displays the main menu available in the Customer Portal, a brief description of each menu item, and a link to the relevant topic in the *Contrail Service Orchestration Customer Portal User Guide*.

[Table 5 on page 8](#) lists the icons on the top right corner of the Customer Portal and a brief description of each icon.

Table 4: Customer Portal Main Menu

Main Menu	Description
Favorites	<p>View the list of pages that you have marked as favorite. You can mark pages that you frequently visit to Favorites.</p> <p>To mark a page as favorites, click the star icon on the right corner of each page.</p>
Dashboard	<p>Access a user-configurable dashboard that you can customize with available widgets (also known as dashlets).</p> <p>For more information, see “About the Customer Portal Dashboard” on page 15.</p>

Table 4: Customer Portal Main Menu (*continued*)

Main Menu	Description
Monitor	<p>Monitor or view the following:</p> <ul style="list-style-type: none"> • Sites: See “About the Monitor Overview Page” on page 808. • Alerts and alarms: See “About the Generated Alerts Page” on page 810 and “About the Alarms Page” on page 817. • Alert definitions and notifications: See “About the Alert Definitions/Notifications Page” on page 812. • Link switchover events (for SD-WAN sites): See “About the SD-WAN Events Page” on page 854. • Security events: See “About the All Security Events Page” on page 823. • Application service-level agreement (SLA) performance (for SD-WAN sites):: See “About the SLA Performance of a Single Tenant Page” on page 856. • Application visibility (for SD-WAN sites): See “About the Application Visibility Page” on page 866. • User visibility: See “About the User Visibility Page” on page 869. • Threat maps: See “About the Threats Map (Live) Page” on page 875. • Jobs (ongoing or completed): See “About the Jobs Page” on page 791.

Table 4: Customer Portal Main Menu (*continued*)

Main Menu	Description
Resources	<p>Manage the following resources:</p> <ul style="list-style-type: none">• Sites: See “About the Site Management Page” on page 68.• Devices: See “About the Devices Page” on page 271.• Deploy or stage images: See “About the Device Images Page” on page 266.• Site groups: See “About the Site Groups Page” on page 216.• Mesh tags: See “About the Mesh Tags Page” on page 241.• Site templates: See “About the Configuration Templates Page” on page 354.• Device templates: See “About the Device Template Page” on page 337.• Configuration templates: See “About the Configuration Templates Page” on page 354.

Table 4: Customer Portal Main Menu (continued)

Main Menu	Description
Configuration	<ul style="list-style-type: none"> • Configure the following: <ul style="list-style-type: none"> • Intent-based firewall policies: See “About the Firewall Policy List Page” on page 443. • Unified threat management (UTM): See “About the UTM Profiles Page” on page 523. • NAT policies: See “About the NAT Policies Page” on page 632. • Intrusion prevention system (IPS): See “About the IPS Signatures Page” on page 665 and “About the IPS Profiles Page” on page 692. • SSL proxy: See “About the SSL Proxy Policy Page” on page 716. • SD-WAN policies: See “About the SD-WAN Policy Page” on page 573. • SLA-based and path-based steering profiles: See “About the SLA-Based Steering Profiles Page” on page 587 and “Adding Path-Based Steering Profiles” on page 602. • SD-WAN breakout profiles: See “About the Breakout Profiles Page” on page 609. • Shared objects (for example, IP addresses): See “About the Addresses Page” on page 751. • View and manage deployments: See “About the Deployments Page” on page 739. • View network services: See “About the Network Services Page” on page 746.
Reports	<ul style="list-style-type: none"> • Add and manage security and SD-WAN report definitions, and generate reports: See “About the Security Report Definitions Page” on page 883 and “About the SD-WAN Report Definitions Page” on page 906. • View generated security and SD-WAN reports: See “About the Security Generated Reports Page” on page 889 and “About the SD-WAN Generated Reports Page” on page 917.

Table 4: Customer Portal Main Menu (*continued*)

Main Menu	Description
Administration	<p>Perform various administrative tasks including the following:</p> <ul style="list-style-type: none"> • Manage users and roles: See “About the Users Page in Customer Portal” on page 36 and “About the Tenant Roles Page” on page 45. • Monitor audit logs: See “About the Audit Logs Page” on page 798. • View device and CSO licenses: See “About the Device Licenses Page” on page 401 and “About the CSO Licenses Page” on page 406. • Modify tenant settings: See “View and Edit Tenant Settings” on page 27. • Install signatures: See “About the Signature Database Page” on page 410. • Manage certificates and VPN authentication: See “About the Certificates Page” on page 417 and “About the VPN Authentication Page” on page 422. • Set up and configure Juniper Identity Management Service (JIMS) See “About the Identity Management Page” on page 433. • Integrate with Mist Access Points (APs): See “Enabling Integration with Mist Access Points” on page 152.

Table 5: Customer Portal Icons

Icons	Description
Running Jobs	<p>Displays the list of jobs that are currently in progress. Click Review All to view the list of all jobs on the Jobs page.</p> <p>For more information on the Jobs page, see “About the Jobs Page” on page 791.</p>
Scheduled Jobs	<p>Displays the list of jobs that are scheduled. Click Review All to view the list of all scheduled jobs on the Jobs page.</p> <p>For more information on the Jobs page, see “About the Jobs Page” on page 791.</p>

Table 5: Customer Portal Icons (*continued*)

Icons	Description
Scope	<p>Displays the scope of a user.</p> <p>If you are an SP administrator or an OpCo administrator, you can change the scope from All Tenants to a specific tenant. For more information on switching the scope, see “Switching the Tenant Scope” on page 13.</p>
Alarms and Alerts	<p>Displays the following two tabs:</p> <ul style="list-style-type: none"> • Alarms—Displays the list of alarms that are generated by the device along with the timestamp and the severity of the alarm. Click Review All to view the details about the generated alarms on the Alarms page. For more information about the Alarms page, see “About the Alarms Page” on page 817. • Alerts—Displays the list of alerts that are generated by the device along with the timestamp and the severity of the alert. Click Review All to view the details about the generated alerts on the Alerts page. For more information about the Alerts page, see “About the Generated Alerts Page” on page 810.
Pending Policies	<p>Displays the list of policies that are due for deployment on the devices managed by CSO. Click Deploy to deploy the policy. The Deploy page appears. Choose the deployment type (Run Now or Schedule at a later time) and click OK.</p> <p>Click Review All to view the details about the pending deployments on the jobs page. See the Awaiting Deployment tab for the list of policies that are due for deployment.</p>
Feedback	<p>Click this icon to provide feedback about the product or report any issues that you are facing.</p>
User Name	<p>Displays the user name of the user who has currently logged into CSO.</p>
Resize	<p>Click this icon to resize the page to full screen.</p>

Table 5: Customer Portal Icons (*continued*)

Icons	Description
Help Menu (?)	<p>Click this icon to access the following panels and online help documentation:</p> <ul style="list-style-type: none"> • Getting Started panel • What's New panel • Quick Help panel • Help Center • Release Notes • About Panel

RELATED DOCUMENTATION

[Accessing Customer Portal | 10](#)
[Changing the Customer Portal Password | 19](#)

Accessing Customer Portal

To access Customer Portal:

1. If you are logging in to Customer Portal for the first time, do the following. If not, skip to [2](#).

NOTE: When your administrator creates a CSO account for you, an e-mail (with the subject line CSO Account Created) is sent. This e-mail contains a URL that allows you to log in to Customer Portal. The URL is active for only 24 hours and is valid only for the first log in.

- a. Click the URL that you have received in the e-mail.

The Change Password page appears with a message that you must change your password for security purposes.

- b. Change your password following the guidelines provided in [Table 6 on page 11](#).
- c. (Optional) Click the Terms of Use link to view the Terms of Use document.

- d. Click the check box to accept CSO terms of use.
- e. Click **Ok**.

The login password is changed and you are logged out of the system. When you log in you must use the changed password.

- 2. Login to Customer Portal using the link provided in the account activation e-mail.

NOTE: We recommend that you use Google Chrome (Version 60 or later) or Firefox (Version 78 or later) to access the Contrail Service Orchestration (CSO) GUI.

- 3. Enter your username (E-mail ID) and password. If two-factor authentication is enabled, you are prompted for a verification code. For information on two-factor authentication, see [“Configuring Two-Factor Authentication” on page 23](#).

The Welcome page appears listing the key features of the release.

- 4. (Optional) If you want to hide the Welcome page on your next login, select the **Hide this on next login** check box.
- 5. (Optional) If you want to review the tenant setting, select **Review Settings**.

The Review Settings page appears. For more information see, [“View and Edit Tenant Settings” on page 27](#).

- 6. Click **Go to Dashboard**. The menu bar on the left-hand side of the every page allows you to access the different tasks easily. The top-level menu items are listed in [Table 7 on page 12](#).

Table 6: Fields on the Change Password Page

Field	Description
New Password	<p>Enter your new password.</p> <p>The password must be between 6 and 21 characters long, and must include at least one lowercase letter, one uppercase letter, one special character, and one number.</p> <p>NOTE: The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.</p>

Table 6: Fields on the Change Password Page (*continued*)

Field	Description
Confirm Password	Reenter the password for confirmation. You can select Show Password to view the password.

Table 7: Customer Portal Menu

Menu Name	Description
Dashboard	Configurable dashboard that offers you a customized view of network services through its widgets
Monitor	Monitor alerts and alarms, security, device, and software-defined WAN (SD-WAN) events; applications and jobs
Resources	Manage device and software image, sites, site templates, mesh tags, and site groups
Configuration	Configure network services, shared objects, and policies (firewall, NAT, SD-WAN), and view and manage configuration deployments
Reports	Create report definitions and view reports
Administration	Manage users, licenses, audit logs, tenant settings, certificate management, Identity Management, and the signature database

RELATED DOCUMENTATION

[Changing the Customer Portal Password | 19](#)

[Customer Portal Overview | 3](#)

Personalize the Customer Portal

You can personalize the navigation mode and the theme in the portal.

To personalize the portal:

1. Click the icon on the lower left corner of the portal. You have an option to personalize the following settings:
 - Navigation Mode
 - Theme
 - Invert colors
2. Select one of the following navigation modes:
 - Side Menu (default option)—Click this option if you want the main menu items to appear on the left pane.
 - Horizontal Menu—Click this option if you want the main menu items to appear horizontally on the top bar.
3. Select one of the following themes:
 - Default—Click this option if you prefer the background color of the portal to be blue.
 - Grey—Click this option if you prefer the background color of the portal to be grey.
4. Enable the toggle button if you prefer to invert the colors.

The changes are immediately applied to the portal.

RELATED DOCUMENTATION

| [Customer Portal Overview](#) | 3

Switching the Tenant Scope

Administration Portal users can change the tenant scope from all tenants to a specific tenant by using the tenant switcher displayed on the banner.

When you switch scope from all tenants to a specific tenant, the menu and pages displayed are almost the same as those displayed for Customer Portal users, with some additional actions visible to the Administration Portal users. When you switch back to the **All Tenants** scope, the menu and pages for the Administration Portal are displayed.

To switch from one scope to another:

- From the top right corner of the page, select the **All Tenants** scope to access Administration Portal or select a specific tenant (for example, aaa) to access Customer Portal. The menu and pages for Administration Portal or Customer Portal are displayed based on the scope selected from the drop-down list.

RELATED DOCUMENTATION

| [Role-Based Access Control Overview](#) | 35

Setting Up Your Network with Customer Portal

Your service provider specifies which sites appear in your network and the network services that you can use. When you start working in Customer Portal, you must set up your network using the available sites and network services.

To set up your network with Customer Portal:

1. You can add the following types of sites from the Sites page:
 - Provider hub site: Connects to multiple spoke sites using overlay connections. To add a provider hub site, see [“Add Provider Hub Sites in SD-WAN Deployments” on page 103](#).
 - Branch site: Represents an endpoint that is part of customer premise equipment (CPE) at some physical location such as branch office or point of sale location. Typically, these points are connected using overlay connections to hub sites. You can add branch sites manually or by using site templates:
 - To manually add a branch site with SD-WAN or Next Gen Firewall capability, see [“Manually Adding Branch Sites” on page 119](#).
 - To add multiple branch sites, use site templates. See [“Add Branch Sites by Using a Site Template” on page 220](#).
 - Cloud spoke site: Connects to a hub site using overlay connections. To add a cloud spoke site, see [“Adding Cloud Spoke Sites for SD-WAN Deployment” on page 105](#).
 - Enterprise hub site: An enterprise hub site carries site-to-site traffic between branch sites and to break out backhaul (central breakout) traffic from branch sites. To add an enterprise hub site, see [“Add Enterprise Hubs with SD-WAN Capability” on page 76](#).
2. Activate the site.

3. Deploy network services. See [“Manage a Site” on page 170](#).
4. View and manage policies.
 - View and manage a firewall policy. See [“Adding Firewall Policy Intents” on page 449](#) and [“Deploying Policies” on page 742](#).
 - View and manage an SD-WAN policy. See [“Adding SLA-Based Steering Profiles” on page 591](#), [“Adding Path-Based Steering Profiles” on page 602](#), [“Creating SD-WAN Policy Intents” on page 575](#), and [“Deploying Policies” on page 742](#).

RELATED DOCUMENTATION

| [Accessing Customer Portal | 10](#)

About the Customer Portal Dashboard

To access the dashboard, select **Customer Portal > Dashboard**.

The user-configurable dashboard that offers you a customized view of network services through its widgets.

You can drag these widgets from the top of the dashboard to your workspace, where you can add, remove, and rearrange them to meet your needs.

The dashboard automatically adjusts the placement of the widgets to dynamically fit on your browser window without changing their order. You can manually reorder the widgets by using the drag and drop option. In addition, you can press and hold the top portion of the widget to move it to a new location.

Tasks You Can Perform

You can perform the following tasks from this page:

- Customize the dashboard by adding, removing, and rearranging the widgets.
- Update the dashboard or an individual widget by clicking the refresh icon.
- Show or hide widget thumbnails in the carousel by selecting the category of widgets that you want to view from the list at the top left of the carousel; the default is **All Widgets**.
- Add a widget to the dashboard by dragging the widget from the palette or thumbnail container into the dashboard.
- Delete a widget from the dashboard page by clicking delete icon (X) in the title bar of the widget and confirming the delete operation.

- Add a dashboard tab by clicking the + icon, (optionally) entering a name, and pressing Enter.

You can then add widgets to the dashboard as needed.

- Rename a dashboard by double-clicking on the title bar of the dashboard, entering a name, and pressing Enter.
- Delete a dashboard by clicking the delete icon (X icon) in the title bar of the dashboard and confirming the delete operation.
- Search for a widget by clicking the search icon (magnifying glass) at the top left of the carousel, entering search text, and pressing Enter.

Field Descriptions

You can quickly view important data by using the widgets at the top of your dashboard.

[Table 8 on page 16](#) describes the dashboard widgets.

Table 8: Widgets on the Customer Portal Dashboard

Widget	Description
Tenant Sites: Total Alerts	<p>Displays the total number of alerts grouped by severity level.</p> <p>Click each alert name to view the total number of tenant sites receiving alerts that are critical, major, or minor.</p>
Top 5 Sites with Alerts	<p>Displays the top five sites in the tenant receiving alerts.</p> <ul style="list-style-type: none"> • Name—Name of the tenant site. • Location—Location of the tenant site. • Status—Type of alerts received: critical, major, or minor.
Top Sites not meeting SLA	<p>Displays a bar chart of the top sites in the tenant that did not meet SLA requirements and the percentage of time that SLA requirements were not met.</p> <p>You can sort the information based on profile and period ranging from the last hour to the last month.</p>
Top Profiles not meeting SLA	<p>Displays a bar chart of the top SLA profiles that did not meet SLA requirements and the percentage of time that SLA requirements were not met.</p> <p>You can sort the information based on location and period ranging from the last hour to the last month.</p>

Table 8: Widgets on the Customer Portal Dashboard (*continued*)

Widget	Description
Top Sites Switching Links	<p>Displays a column chart of the top sites in the tenant that switched WAN links to meet SLA requirements and the number of link-switch events for the sites.</p> <p>You can sort the information based on profile and period ranging from the last hour to the last month.</p>
Top Profiles Switching Links	<p>Displays a column chart of the top SLA profiles that switched WAN links and the number of link-switch events for the SLA profiles.</p> <p>You can sort the information based on location and period ranging from the last hour to the last month.</p>
Top Applications by Throughput	<p>Displays a bar chart of the top sites in the tenant that did not meet SLA requirements and the percentage of time that SLA requirements were not met.</p> <p>You can sort the information based on profile, location, and time period.</p>
Firewall: Top Denials	<p>Displays a column chart of the top requests denied by the firewall based on their source IP addresses, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
Firewall: Top Events	<p>Displays a bar chart of the top firewall events of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IPS: Top Events	<p>Displays the top IPS events of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
Applications: Top by Sessions	<p>Displays a bar chart of the top applications with a maximum number of sessions, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IP: Top Destinations	<p>Displays the top IP destination addresses of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IP: Top Sources	<p>Displays the top IP source addresses of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>

Table 8: Widgets on the Customer Portal Dashboard (*continued*)

Widget	Description
IP: Top Spams by Source IPs	<p>Displays the number of spams detected by the source IPs.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
Virus: Top Blocked	<p>Displays viruses with the maximum number of blocks, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
Web Filtering: Top Blocked Websites	<p>Displays a bar chart of websites with the maximum number of blocks, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IP: Top Source IPs by Volume	<p>Displays the top source IP addresses based on volume of traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 15 minutes to 7 days.</p>
Application: Top Application by Volume	<p>Displays the applications based on volume of traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days and view the information in a bar chart or a bubble chart.</p>
IP: Top Users/IP by Sessions	<p>Displays the top source IP addresses by sessions, sorted by count.</p> <p>You can sort the information based on time period ranging from 15 minutes to 7 days.</p>
Threat Map: Virus	<p>Displays a world map showing total virus event count across countries.</p> <p>You can sort the information based on source, destination, and time period ranging from 5 minutes to 7 days.</p>
Threat Map: IPS	<p>Displays a world map showing total IPS event count across countries.</p> <p>You can sort the information based on source, destination, and time period ranging from 5 minutes to 7 days.</p>

RELATED DOCUMENTATION

[Customer Portal Overview](#) | 3

Changing the Customer Portal Password

To change the Customer Portal password:

1. Click the customer username that is located at the right side of the Customer Portal banner.
The drop-down list appears.
2. Click **My Profile**. Alternatively, you can access the My Profile page from **Administration > My Profile**.
The My Profile page appears.

3. Click **Change Password**.

4. Enter the current password.

5. In the New Password text box, specify your new password.

The login password that you set must conform to a particular set of requirements such as minimum length of 6 characters, a maximum length of 21 characters, and that includes at least one lowercase letter, one uppercase letter, an alpha-numeric character, and a numeric character.

You must change the password periodically (every 90 days) and you cannot reuse the old password. Your user account will be locked after five consecutive unsuccessful login attempts.

6. In the Confirm Password text box, specify your new password again.

7. Click **Save**.

You are logged out of the system. To log in to Customer Portal again, you must use your new password. Other sessions logged in with the same username are unaffected until the next login.

RELATED DOCUMENTATION

[Customer Portal Overview](#) | 3

[Accessing Customer Portal](#) | 10

Resetting the Password

If you have forgotten your password, you can reset the password from the Contrail Service Orchestration (CSO) login page.

NOTE: If you have entered an incorrect password, your account will be locked after five consecutive unsuccessful login attempts.

To reset the password:

- 1. On the login page, enter the username , and then press **Enter**.
- 2. Click the **Forgot Password** link.

The Forgot Password page appears, with a message that an e-mail notification with a verification code is sent to your e-mail address.

NOTE: The **Forgot Password** link appears only after you specify the username.

- 3. In **Verification Code**, specify the verification code that you have received through an e-mail.

NOTE: The verification code expires after a time duration of 15 minutes.

- 4. Click **OK**.

The Reset Password page appears.

- 5. Change your password following the guidelines provided in [Table 9 on page 20](#).
- 6. Click **OK**.

Your password is reset.

Table 9: Fields on the Reset Password Page

Field	Description
Username	Enter your username.

Table 9: Fields on the Reset Password Page (*continued*)

Field	Description
New Password	<p>Enter your new password.</p> <p>The login password that you set must be between 6 and 21 characters long, and it must include at least one lowercase letter, one uppercase letter, one special character, and one number.</p> <p>NOTE: The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.</p>
Confirm Password	<p>Reenter the password for confirmation.</p> <p>You can select Show Password to view the password.</p>

RELATED DOCUMENTATION

[Accessing Customer Portal | 10](#)
[Changing the Password on First Login | 21](#)
[Changing the Customer Portal Password | 19](#)

Changing the Password on First Login

To enhance the security related to login credentials, you are prompted to change the password when you login to the portal for the first time.

To change the password when you log in for the first time:

1. Log in to the portal with the default login credentials.

The Change Password page appears with a message that you must change your password for security purposes.

NOTE: The Change Password page appears only if you are logging in to the portal for the first time.

2. Change your password following the guidelines provided in [Table 6 on page 11](#).

- 3. (Optional) Click the Terms of Use link to view the Terms of Use document
- 4. Click the check box to accept CSO terms of use.
- 5. Click **Ok**.

NOTE: It is mandatory to change the password when you log in to the portal for the first time. If you click **Cancel**, you are redirected to the login page.

The login password is changed and you are logged out of the system. When you log in you must use the changed password.

Table 10: Fields on the Change Password Page

Field	Description
New Password	<p>Enter your new password.</p> <p>The password must be between 6 and 21 characters long, and must include at least one lowercase letter, one uppercase letter, one special character, and one number.</p> <p>NOTE: The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.</p>
Confirm Password	<p>Reenter the password for confirmation.</p> <p>You can select Show Password to view the password.</p>

RELATED DOCUMENTATION

Accessing Customer Portal 10
Changing the Customer Portal Password 19
Resetting the Password 19

Set a New Password After Your Existing Password Expires

Once the specified password duration (in days) expires, you must set a new password to log in to Contrail Service Orchestration (CSO).

NOTE: By default, the password expiration duration is 180 days. However, you can change the expiration duration while onboarding the tenant.

When you try to log in to CSO with your expired credentials and click **Login**, a set password dialog box appears.

To set a new password:

1. In the **Password** field, specify your new password.

The login password that you set must conform to a particular set of requirements such as minimum length of 6 characters, a maximum length of 21 characters, and that includes at least one lowercase letter, one uppercase letter, an alpha-numeric character, and a numeric character. You must change the password periodically (every 180 days) and you cannot reuse the old password. Your user account will be locked after five consecutive unsuccessful login attempts.

2. In the **Confirm Password** field, specify your new password again.

You can select the show password (eye) icon to view the password you entered.

3. Click **OK**.

You are redirected to the CSO login page where you must enter the newly updated credentials to log in to CSO.

WHAT'S NEXT

After setting the new password, to log in to CSO, see [Accessing Customer Portal | 10](#).

RELATED DOCUMENTATION

[View and Edit Tenant Settings | 27](#)

[Customer Portal Overview | 3](#)

Configuring Two-Factor Authentication

Two-factor authentication adds an additional authentication level for enhanced login security. CSO uses username and password as the first level of user verification. Starting from Release 6.1.0, CSO supports

configuring an optional second level of verification. The second level of verification mandates a user to authenticate through a verification code either sent through an e-mail (default option) or generated using an authentication server.

By default, two-factor authentication is disabled for all users. SP and OpCo administrators can enable or disable two-factor authentication in the Authentication page (**Administration > Authentication**), whereas tenant administrators can perform the same in the Tenant Settings page (**Administration > Tenant Settings**).

- If an administrator enables two-factor authentication at the global, OpCo, or tenant-level, then all existing and new users under that level are automatically configured for two-factor authentication. For example, if an OpCo administrator enables two-factor authentication, then all the users under that OpCo are configured for two-factor authentication.

Individual users cannot disable two-factor authentication if it is enabled by the administrator. However, users can change the authentication method. The default authentication mechanism is e-mail OTP.

- If two-factor authentication is disabled at the global, OpCo, or tenant-level, then individual users can choose to enable two-factor authentication. Users can also change the authentication mechanism.

For example, if two-factor authentication is disabled at the tenant-level, then tenant users are required to enter only the username and password to log into CSO. If individual users under that tenant want to use an additional verification level, then they can choose to enable two-factor authentication in the My Profiles page.

- If the administrator enables two-factor authentication initially and then later disables it, then existing users continue to have two-factor authentication enabled. Existing users can opt to disable two-factor authentication in the My Profile page (**Administration > My Profile**).

However, two-factor authentication is disabled for new users. New users can enable two-factor authentication based on individual requirements.

Individual users can enable two-factor authentication if it is disabled. Users cannot disable two-factor authentication if it is enabled by the administrator.

NOTE: If single sign-on (SSO) is enabled at the global or OpCo level, administrators cannot enable two-factor authentication for the users at that level.

1. Select **Administration > My Profile**.

The My Profile page appears.

NOTE: If SSO is enabled in any of the scopes that the user is part of, then the My Profile page displays only the username as the user credentials are managed by the SSO server.

2. Click the toggle button to enable two-factor authentication.

CSO provides two methods for two-factor authentication—e-mail and TOTP authentication. E-mail is the default method. You can opt to select TOTP authentication.

To enable TOTP authentication:

1. Install a Time-Based One-Time Password (TOTP) authenticator application on your mobile phone. You can use a TOTP authenticator application such as Authy, Duo Mobile, or you can use an authenticator from Microsoft, LastPass, or Google.
2. Scan the QR code provided in the My Profile page using the authenticator application to register your mobile phone with CSO.
3. Enter the verification code generated by the authenticator application and click **Verify**.

After CSO verifies the code, TOTP authentication is enabled. When you log in to CSO, you are prompted for a verification code that is generated by the authenticator application.

If you change your mobile phone, click **Change Phone** to unregister the existing phone from CSO. To register the new phone with CSO, follow steps 1 through 3.

If you do not want to use the TOTP authentication method, click **Delete**.

Extending the User Login Session

In the unified portal, a login session expires in 60 minutes. After 55 minutes, the **Extend Session** page is displayed and, prompting you to enter your password. You must enter your password to extend the session. The **Extend Session** page is displayed when the **Local** authentication method is configured.

If you have logged in to the portal with SSO authentication, the **Extend Session** page is displayed and you can authenticate with the external SSO server. However, the SSO expiration is not under the control of CSO and the following can happen:

- If the external SSO session is expired, you will be authenticated in the **Extend Session** page. After successful authentication, the **Extend Session** page is closed automatically.
- If the external SSO session is not expired, the **Extend Session** page is closed automatically.

To extend the login session:

1. On the **Extend Session** page, enter your password in the **Password** field. If you want to end your session and exit from the portal, click **Cancel** instead and you are redirected to the Login page.

2. Click **OK**.

The success message **Your Session has been successfully extended** is displayed.

RELATED DOCUMENTATION

[Changing the Customer Portal Password | 19](#)

Resend Activation Link in Customer Portal

When tenant administrators adds a new user with tenant administrator or operator roles, CSO automatically sends an activation link to their e-mail account. The tenant administrator can resend activation link to the user's account in the following events:

- The initial activation link expired, or
- The e-mail with the activation link does not get delivered, or
- The user's account must be manually re-enabled.

To resend the activation link:

1. Select **Administration > Users** in Customer Portal.

The Users page appears, displaying a list of users.

2. Select the username to whose account you want to send the activation link, and then select **More > Resend Activation Link**.

An alert message appears, asking you to confirm the resend activation link operation.

3. Click **Yes** to confirm the resend activation link operation.

An e-mail is sent to the user's e-mail address with a URL to reset the password in order to activate their account in CSO. The URL is active for 24 hours.

RELATED DOCUMENTATION

[Resetting the Password for Tenant Users | 41](#)

[Adding Tenant and OpCo Tenant Users | 38](#)

[Adding User-Defined Roles for Tenant Users | 46](#)

View and Edit Tenant Settings

Users with a tenant administrator role can view and modify the tenant settings that are configured on the Administration Portal, while users with tenant operator role can only view the tenant settings.

NOTE: You cannot add or remove services (configured in Administration Portal) for the tenant.

To modify the settings configured for a tenant:

1. If the Welcome to CSO *Release-Number* page is displayed after you log in, click **Review Settings**. Alternatively, select **Administration > Tenant Settings**.

The Tenant Settings page appears.

2. (Optional) Click the Expand icon or the Collapse icon on the top-right corner of the page to expand or collapse the different sections displayed.

3. Modify the tenant settings as explained in [Table 11 on page 28](#).

4. Click **Save** to save the changes.

A tenant edit job is triggered and a confirmation message, indicating that a tenant edit job is created successfully, appears on the Tenant Settings page.

5. (Optional) You can click the job name in the message to view details of the job (including job status, start date and time, and end date and time) on the **Update tenant settings Details** page. Alternatively, you can view the status of the job on the Jobs (**Monitor > Jobs**) page.

If the job is completed successfully, a confirmation message appears on top of the Tenant Settings page.

Table 11: Fields on the Tenant Settings Page

Field	Description	Tenant Capabilities (Services)
Services	Displays the services supported for the tenant You cannot modify this setting.	SD-WAN (Advanced or Essential) Security Services (Next Gen Firewall)
<i>Password Policy</i>		SD-WAN Next Gen Firewall
Password Expiration Days	Specify the duration (in days) after which the password expires and must be changed. Range: 1 through 365. Default: 180 days. NOTE: The modifications are applicable only to new users and users whose password has expired.	SD-WAN Next Gen Firewall
<i>Two-Factor Authentication</i>		
Two-Factor Authentication	Click the toggle button to either enable or disable two-factor authentication for all tenant users. <ul style="list-style-type: none"> • If you enable two-factor authentication, then individual users cannot disable it. • If two-factor authentication is disabled, then individual users can enable it from the Administration > My Profile page. <p>If the administrator enables two-factor authentication initially and then later disables it, then existing users continue to have two-factor authentication enabled. Existing users can opt to disable two-factor authentication in the My Profile page (Administration > My Profile).</p> <p>However, two-factor authentication is disabled for new users. New users can enable two-factor authentication from the My Profile page if required.</p>	SD-WAN Next Gen Firewall

Table 11: Fields on the Tenant Settings Page (*continued*)

Field	Description	Tenant Capabilities (Services)
SSL Settings	<p>NOTE: You can modify this setting only if you have not added any SD-WAN sites for the tenant.</p>	SD-WAN
Default SSL Proxy Profile	<p>Click the toggle button to enable or disable a default SSL proxy profile for the tenant.</p> <p>If you enable this option, the following items are created:</p> <ul style="list-style-type: none"> • A default root certificate with the certificate content specified (in the Root Certificate field) • A default SSL proxy profile • A default SSL proxy profile intent that references the default profile <p>NOTE: You use this option to create a tenant-wide default profile; enabling or disabling this option does <i>not</i> mean that SSL is enabled or disabled.</p> <p>If you enable this option, you must add a root certificate.</p>	SD-WAN

Table 11: Fields on the Tenant Settings Page (*continued*)

Field	Description	Tenant Capabilities (Services)
Root Certificate	<p>NOTE: This field is displayed only if you enabled the default SSL proxy profile.</p> <p>You can add a root certificate (X.509 ASCII format) by importing the certificate content from a file or by pasting the certificate content:</p> <ul style="list-style-type: none"> To import the certificate content directly from a file: <ol style="list-style-type: none"> Click Browse. <p>The File Upload dialog box appears.</p> <ol style="list-style-type: none"> Select a file and click Open. <p>The content of the certificate file is displayed in the Root Certificate field.</p> Copy the certificate content from a file and paste it in the text box. <p>After the tenant is successfully added, a default root certificate, a default SSL proxy profile, and a default SSL proxy profile intent are created.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The root certificate must contain both the certificate content and the private key. For full-fledged certificate operations, such as certificates that need a passphrase, or that have RSA private keys, you must use the Certificates page (Administration > Certificates) to import the certificates and install on one or more sites. 	SD-WAN
VPN Authentication		SD-WAN

Table 11: Fields on the Tenant Settings Page (*continued*)

Field	Description	Tenant Capabilities (Services)
Authentication Type	<p>NOTE:</p> <ul style="list-style-type: none"> • If PKI Certificate was configured as the authentication type, you can modify the PKI properties (CA Server URL, Password, CRL Server, and Auto Renew) even after you add sites for the tenant. • If Preshared Key was configured as the authentication type, then you can modify the authentication type only if you have not added SD-WAN sites for the tenant. <p>Select the VPN authentication method to establish a secure IPsec tunnel:</p> <ul style="list-style-type: none"> • Preshared Key, which means that CSO establishes IPsec tunnels using keys. • PKI Certificate, which means that CSO establishes IPsec tunnels using public key infrastructure (PKI) certificates. <p>If you select this option, you can configure the following:</p> <ul style="list-style-type: none"> • CA Server URL—Specify the Certificate Authority (CA) Server URL. For example, <code>http://CA-Server-IP-Address/certsrv/mscep/mscep.dll/pkiclient.exe</code>. • Password—Specify the password for the CA server. This field is optional. • CRL Server URL—Specify the certificate revocation list (CRL) server URL. For example, <code>http://Revocation-List-Server-IP-Address/certservices/abc.crl</code>. CSO retrieves the list of revoked certificates from the CRL server. • Auto Renew CA Certificates—Click the toggle button to enable or disable automatic renewal of certificates. If you enable this option, certificates are automatically renewed for all sites in the tenant. If you disable this option, certificates must be manually renewed. <p>NOTE: If the certificate expires before the renewal, CSO might not be able to reach the device.</p> <ul style="list-style-type: none"> • Renew before expiry—If you enabled automatic renewal, select the period (3 days, 1 week, 2 weeks, or 1 month) before the expiration date when the certificates get automatically renewed. <p>NOTE: You can also change the duration in the VPN Authentication page in Customer Portal (Administration > Certificate Management > VPN Authentication) page.</p>	SD-WAN
Overlay Tunnel Encryption	<p>NOTE: You can modify this setting only if you have not added any SD-WAN sites for the tenant.</p>	SD-WAN

Table 11: Fields on the Tenant Settings Page (*continued*)

Field	Description	Tenant Capabilities (Services)
Encryption Type	<p>For security reasons, all data that passes through the VPN tunnel must be encrypted. Select the encryption type:</p> <ul style="list-style-type: none"> • 3DES-CBC—Triple Data Encryption Standard with Cipher-Block Chaining (CBC) algorithm. • AES-128-CBC—128-bit Advanced Encryption Standard with CBC algorithm. • AES-128-GCM—128-bit Advanced Encryption Standard with Galois/Counter Mode (GCM) algorithm. • AES-256-CBC—256-bit Advanced Encryption Standard with CBC algorithm. • AES-256-GCM—256-bit Advanced Encryption Standard with GCM algorithm. <p>The default encryption type is AES-256-GCM.</p>	SD-WAN
<i>Network Segmentation</i>	NOTE: You can modify this setting only if you have not added any SD-WAN sites for the tenant.	SD-WAN
Network Segmentation	Click the toggle button to disable network segmentation on the tenant.	SD-WAN
<i>Dynamic Mesh</i>	<p>NOTE:</p> <ul style="list-style-type: none"> • You can modify these settings even after you add sites for the tenant. • Sites with SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. 	SD-WAN
Threshold for Creating a Tunnel	Not applicable to sites with SD-WAN Essentials service.	SD-WAN
Number of Sessions	<p>Specify the maximum number of sessions closed (for a time duration of 2 minutes) between two branch sites.</p> <p>The dynamic mesh tunnel is created between two branch sites if the number of sessions closed (for a time duration of 2 minutes) is greater than or equal to the value that you specified.</p> <p>The default threshold value (the number of sessions for 2 minutes) is 5.</p>	SD-WAN
<i>Threshold for Deleting a Tunnel</i>	Not applicable to sites with SD-WAN Essentials service.	SD-WAN

Table 11: Fields on the Tenant Settings Page (*continued*)

Field	Description	Tenant Capabilities (Services)
Number of Sessions	<p>Specify the minimum number of sessions closed (for a time duration of 15 minutes) between two branch sites.</p> <p>The dynamic mesh tunnel is deleted between two branch sites if the number of sessions closed (for a time duration of 15 minutes) is lesser than or equal to the value that you specified.</p> <p>The default threshold value (the number of sessions for 15 minutes) is 2.</p>	SD-WAN
<i>Max Dynamic Mesh Tunnels</i>		SD-WAN
Max tunnels per CSO	<p>Displays the maximum number of dynamic mesh tunnels that can be created in CSO. The total number of dynamic mesh tunnels that can be created by all tenants in CSO is limited to 125000.</p> <p>You cannot modify this field.</p>	SD-WAN
Max tunnels per tenant	<p>Specify the maximum number of dynamic mesh tunnels that the tenant can create.</p> <p>Range: 1 through 50,000.</p>	SD-WAN
Dynamic Mesh	Click the toggle button to disable or enable dynamic meshing between sites in the tenant.	SD-WAN
<i>Cloud Breakout Settings</i>	NOTE: You can modify these settings even after you add sites for the tenant.	SD-WAN
Customer Domain Name	Enter the domain name of the tenant. The domain name is used in cloud breakout profiles to generate the fully qualified domain name (FQDN). The cloud security providers use the FQDN to identify the IPsec tunnels.	SD-WAN

Table 11: Fields on the Tenant Settings Page (*continued*)

Field	Description	Tenant Capabilities (Services)
<i>Tenant-Specific Attributes</i>	<p>NOTE: You can modify these settings even after you add sites for a tenant.</p> <p>If you have set up a third-party provider edge (PE) device by using software other than CSO, then configure settings on that router by specifying custom parameters and its corresponding values.</p> <p>You can modify existing attributes or add attributes.</p> <ul style="list-style-type: none"> To add an attribute: <ol style="list-style-type: none"> Click the add (+) icon. An editable row appears inline in the table. Specify any information about the site that you want to pass to a third-party router; for example, location. Specify a value for the information about the site that you want to pass to a third-party device; for example, Chicago. Click ✓ (check mark) to save your changes. The prefix that you entered is displayed in the table. To modify an attribute, select a row, click the edit (pencil) icon, and modify the name and value. 	SD-WAN Next Gen Firewall

RELATED DOCUMENTATION

[About the Site Management Page](#) | 68

Users and Roles

IN THIS CHAPTER

- [Role-Based Access Control Overview | 35](#)
- [About the Users Page in Customer Portal | 36](#)
- [Adding Tenant and OpCo Tenant Users | 38](#)
- [Editing and Deleting Tenant and OpCo Tenant Users | 40](#)
- [Resetting the Password for Tenant Users | 41](#)
- [Roles Overview | 42](#)
- [About the Tenant Roles Page | 45](#)
- [Adding User-Defined Roles for Tenant Users | 46](#)
- [Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 47](#)
- [Access Privileges for Role Scopes \(Tenant and Operating Company\) | 50](#)

Role-Based Access Control Overview

Contrail Service Orchestration supports the authentication and authorization of users. Both service provider and tenant users access the pages within the unified Administration and Customer Portal based on their role and access permissions.

In addition to predefined roles, CSO enables you to add object-based custom roles. You can create custom roles and assign access privileges (read, create, update, delete, and other actions) to each role.

[Table 12 on page 35](#) shows predefined service provider, tenant, and OpCo roles and their access privileges.

Table 12: Roles and Access Privileges

Role	Role Scope	Access Privileges
Tenant Admin	Tenant	Users with the Tenant Admin role have full access to the Customer Portal UI and APIs. They can add one or more users with the Tenant Administrator or Tenant Operator roles.

Table 12: Roles and Access Privileges (*continued*)

Role	Role Scope	Access Privileges
Tenant Operator	Tenant	Users with the Tenant Operator role have read-only access to the Customer Portal UI and APIs.
OpCo Admin	Operating Company	Users with the OpCo Admin role have full access to the OpCo's Administration Portal UI or API capabilities. They can use the UI or APIs to add one or more users with OpCo Admin, OpCo Operator, and custom roles. They can onboard tenants, and add the first tenant user during the OpCo's tenant onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant.
OpCo Operator	Operating Company	Users with the OpCo Operator role have read-only access to the OpCo's Customer Portal UI and APIs.

RELATED DOCUMENTATION

[About the Users Page in Customer Portal](#) | 36

About the Users Page in Customer Portal

To access the Users page for a tenant or OpCo tenant, click **Administration > Users** in the Customer Portal.

Use this page to manage tenants and OpCo tenant users in the Tenant and OpCo scopes respectively. In the Tenant scope, the SP Admin, SP Operator, Tenant Admin, and Tenant Operator can access the Users page for tenants. The SP Admin and the SP Operator can switch scope from all tenants to a specific tenant.

In the OpCo scope, the SP Admin, SP Operator, OpCo Admin and OpCo Operator can access the OpCo Tenant Users page.

For information about the predefined roles and access permissions of OpCo tenant users and tenant users, see *Role-Based Access Control Overview*.

The information listed on the Users page changes depending on the authentication mode configured:

- **Local Authentication** —The **Users** page lists local users that you can add, edit, and delete.
- **Authentication and Authorization with SSO Server**—The **Users** page is not displayed because users are externally managed in the single sign-on (SSO) server.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a tenant user or an OpCo tenant user. See [“Adding Tenant and OpCo Tenant Users” on page 38](#).
- Edit or delete a tenant user or an OpCo tenantuser. See [“Editing and Deleting Tenant and OpCo Tenant Users” on page 40](#).
- View details of users in the respective scope. See [Table 13 on page 37](#).
- Show or hide columns about users. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a user. Click the Search icon in the top right corner of the page to search for a user.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

[Table 13 on page 37](#) describes the fields on the Users page for the Tenant and OpCo scopes in the Customer Portal.

Table 13: Fields on the Users Page

Field	Description
Username	Username of the user. Example: <i>abc@example.com</i>
First Name	First name of the user.
Last Name	Last name of the user.
Status	Indicates whether the user is enabled (can log in to CSO) or disabled (cannot log in to CSO).
Role	Depending on the scope selected, indicates the roles assigned to the tenant or OpCo tenant user. By default, this column lists only one role assigned to the user. When a user is assigned more than one role, a +<integer> icon (for example: +2) appears to the right of the role. The integer indicates the number of additional roles assigned to the user. Click on the integer to view the additional roles.

Table 13: Fields on the Users Page *(continued)*

Field	Description
Last Login	Date and time of the last login. The format is MM/DD/YYYY HH:MM. Example: 07/22/2017 20:07 A date and time is not displayed when a user has not logged in to the Customer Portal.

RELATED DOCUMENTATION

| [Switching the Tenant Scope](#) | 13

Adding Tenant and OpCo Tenant Users

Use the Add Tenant User page and Add OpCo Tenant User page in the Customer Portal to add tenant users and OpCo tenant users respectively to Contrail Service Orchestration (CSO). After you add a user, the user receives an e-mail with the initial login credentials.

NOTE: To add users, you should be assigned a role, such as Tenant Admin, that allows you to add users.

To add a tenant user or an OpCo tenant user:

1. Select **Administration > Users**.

The Users page appears.
2. Click the add icon (+) or click **Add User button**. The Add User button appears when there are no users configured in the scope.

In the Tenant scope, the Add Tenant User page appears. In the OpCo scope, the Add OpCo Tenant User page appears.
3. Complete the configuration as described in [Table 14 on page 39](#).
4. Click **OK** to save the changes. If you want to discard the changes, click **Cancel**.

If you click OK, a confirmation message indicating that the user account is created appears and the user account is listed on the Users page.

To enhance the security related to login credentials, an automatically generated password is sent to the e-mail address that you have specified for the user. You are prompted to change the password when you login to the portal with the automatically generated password. For more information about changing the password on first login, see [“Changing the Password on First Login” on page 21](#).

Table 14: Fields on the Add Tenant User and Add OpCo Tenant User Pages

Field	Description
First Name	Enter the first name as a string of alphanumeric characters, some special characters [underscore (_) and period(.)], and spaces. The maximum length allowed is 32 characters.
Last Name	Enter the last name as a string of alphanumeric characters, some special characters [underscore (_) and period(.)] and spaces. The maximum length allowed is 32 characters.
Username (E-mail)	Enter a valid e-mail address in the <i>user@domain</i> format.
Status	<p>Click the toggle button to enable or disable the user.</p> <p>By default, the status is enabled. A user can log in to CSO only when the status is enabled.</p>
Role	<p>Select one or more roles (both predefined and custom) that you want to assign to the tenant or OpCo tenant user.</p> <p>The following predefined roles are available—Tenant Operator, Tenant Admin, and ConfigureSite. To know more about the predefined roles for tenant users and OpCo tenant users, see <i>Role-Based Access Control Overview</i>.</p> <p>Click the right-arrow icon to move the selected roles from the Available column to the Selected column. Note that you can use the search icon on the top right of each column to search for role names.</p> <p>Click the role name to preview the access privileges assigned to the tenant user.</p>

Editing and Deleting Tenant and OpCo Tenant Users

IN THIS SECTION

- [Editing Tenant and OpCo Tenant Users | 40](#)
- [Deleting Tenant and OpCo Tenant Users | 41](#)

You can edit the information of tenant and OpCo tenant users and delete one or more users.

NOTE: To edit and delete users, you should be assigned a role, such as Tenant Admin, that allows you to edit and delete users.

Editing Tenant and OpCo Tenant Users

To modify a tenant user or an OpCo tenant user:

1. Select **Administration > Users**.

The Users page appears.

2. Select the user that you want to modify, and click the edit icon.

In the Tenant scope, the Edit Tenant User page appears. In the OpCo scope, the Edit OpCo Tenant User page appears.

3. Modify the parameters following the guidelines provided in [Table 14 on page 39](#).

NOTE: You cannot modify the **Username (E-mail)** field.

4. Click **OK** to save the changes or click **Cancel** to discard your changes.

If you click OK, a confirmation message indicating that the user information is modified appears on top of the Users page.

Deleting Tenant and OpCo Tenant Users

To delete one or more tenant users and OpCo tenant users:

1. Select **Administration > Users**.

The Users page appears.

2. Select the users that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the users or click **No** to cancel the deletion.

If you click **Yes**, a confirmation message indicating that the selected users account are deleted from CSO appears on top of the Users page.

Resetting the Password for Tenant Users

Users with the Tenant Administrator role can reset the password for tenant users. Also, users with the Update capability for Users objects can reset the password for tenant users.

To reset the password:

1. Select **Administration > Users** in Customer Portal.

The Users page appears, displaying a list of tenant users.

2. Select the username for which you want to reset the password, and then select **More > Reset Password**.

An alert message appears, asking you to confirm the reset password operation.

3. Click **Yes** to confirm the reset password operation.

A confirmation message appears, indicating that the password has been successfully reset, and an e-mail with a new system-generated password is sent to the user.

The user can use the new system-generated password to log in to CSO.

RELATED DOCUMENTATION

| [About the Users Page in Customer Portal](#) | 36

Roles Overview

IN THIS SECTION

- [Types of Roles | 42](#)
- [Role Scopes | 43](#)
- [Access Privileges | 43](#)
- [Relationship Between User, Roles, and Access Privileges | 43](#)
- [Benefits of role-based access control \(RBAC\) | 44](#)

A role is a function assigned to a user that defines the tasks that the user can perform within CSO. Each user can be assigned one or more roles depending on the tasks that the user is expected to perform.

User roles enable you to classify users based on the privileges to perform tasks on CSO objects. Roles assigned to a user determine the tasks and actions that the user can perform.

This topic contains the following sections:

Types of Roles

There are two types of roles: predefined roles and custom roles.

- **Predefined roles**—System-defined roles with a set of predefined access privileges assigned to a user to perform tasks within the CSO application. Predefined roles are created in the system during CSO installation. For more information about predefined roles, see *Role-Based Access Control Overview*.
- **Custom roles**—Object-based user-defined roles with a set of access privileges assigned to a user to perform tasks within the CSO application. Objects include menu and submenu items (for example, Resources, Devices, Images, and POPs) in the CSO application, from which you can create, edit, clone, and delete objects.

Custom roles can be created by:

- An OpCo Administrator, or a Tenant Administrator.
- A tenant user with the Create Role privilege. This user can create custom roles for tenant users.
- An OpCo user with the Create Role privilege. This user can create custom roles for both OpCo and tenant users.

You can create custom roles and assign access privileges to each role by using the Roles page (**Administration > Roles**).

You can assign one or more roles to a user when you create or edit a user account. Each role can have one or more access privileges.

Role Scopes

A role scope defines the specific scope, which is assigned to the role, such as service provider, OpCo, or tenant. An OpCo Administrator can assign OpCo, and tenant roles to OpCo users and tenant roles to tenant users. A Tenant Administrator can assign tenant roles only to tenant users. A role can have the following scopes:

- **Tenant**—Represents a customer that can view, configure, and manage its sites through Customer Portal.
- **Operating Company (OpCo)**—Similar to a service provider that can manage its own tenants. Tenants managed by one OpCo are isolated from tenants of another OpCo. An OpCo can manage all activities related to its own tenants.

Access Privileges

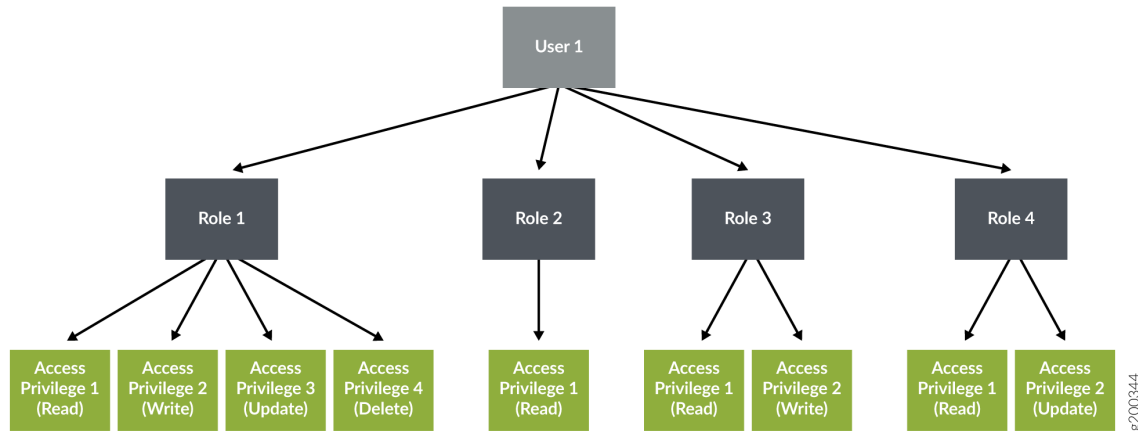
The following access privileges and actions can be assigned to a user role:

- Read
- Create
- Update
- Delete
- Other actions (Example: For device templates object, the following other actions are supported: Clone and Edit Device Template) .

Relationship Between User, Roles, and Access Privileges

[Figure 1 on page 44](#) shows the relationship between a user, user roles, and access privileges. A user can have one or more roles and each role can have one or more access privileges.

Figure 1: Relationship Between User, Roles, and Access Privileges



Benefits of role-based access control (RBAC)

- CSO provides pre-defined and user-defined set of roles for day-to-day system operations on the unified Administration and Customer portal.
- Controls which system users can view, read, write, and execute objects based on certain business and operation needs.
- Provides granular level access control on CSO objects within each navigation menu.
- Helps service providers in upselling advanced features to their tenants as a power user.
- CSO supports RBAC and authenticate users using local authentication and the external Single Sign On (SSO) server.

RELATED DOCUMENTATION

[About the Tenant Roles Page | 45](#)

[Adding User-Defined Roles for Tenant Users | 46](#)

[Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 47](#)

About the Tenant Roles Page

To access this page, select **Administration > Roles** in the Customer Portal.

You can use the Roles page to view a list of predefined (system-defined) and custom (user-defined) roles that can be assigned to tenant users. You can create, edit, or delete custom roles and clone both custom and predefined roles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a custom role for the tenant users. See [“Adding User-Defined Roles for Tenant Users” on page 46](#).
- Edit, clone, or delete a custom role. See [“Editing, Cloning, and Deleting User-Defined Roles for Tenant Users” on page 47](#).

Field Descriptions

[Table 15 on page 45](#) describes the fields on the Roles page.

Table 15: Fields on the Roles Page

Field	Description
Role Name	Displays the name of the role.
Role Scope	Displays the scope of the role.
Role Type	Displays whether the role is a predefined role or a custom role.
Created By	Displays the name of the user that created the role.

RELATED DOCUMENTATION

[Roles Overview | 42](#)

[Role-Based Access Control Overview | 35](#)

[Adding User-Defined Roles for Tenant Users | 46](#)

[Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 47](#)

Adding User-Defined Roles for Tenant Users

Use the Add Role page to create custom (user-defined) roles and assign access privileges (read, create, update, delete, and other actions) to the tenant user roles.

A Tenant Administrator or a user with the Create Role privilege can create custom roles for tenant users.

To create a custom role:

1. Select **Administration > Roles** in Customer Portal.

The Roles page appears.

2. Click the add icon (+) to create a new role.

The Add Role page appears.

3. Complete the configuration according to the guidelines provided in [Table 16 on page 46](#).

4. Click **OK**.

A new role is created and listed on the Roles page.

Table 16: Fields on the Add Role Page

Field	Description
Role Name	Enter a unique role name. The name can contain alphanumeric characters, underscore, period, and space.
Description	Enter a description for the role.
Role scope (Visibility)	Select the scope of the role. If you select the scope as Tenant, then the Privileges section of the page displays all the objects of Customer Portal.

Table 16: Fields on the Add Role Page (continued)

Field	Description
Privileges	<p>All Objects—Displays the objects of the Customer Portal. You must select the check box against each object and then select the type of privileges (read, create, update, delete, and other actions (schedule, deploy, reboot, activate, retry, schedule update, schedule delete, and so on)) that you want to assign the user for the selected object. You can select one or more access privileges to assign to the tenant user role.</p> <p>NOTE: You must assign at least one access privilege to a role.</p> <p>If you select the first-level objects, the submenu items that belong to the main object and the corresponding access privileges are selected by default.</p> <p>The following access privileges can be assigned to a user role:</p> <ul style="list-style-type: none">• Read—Enables the user to read existing objects.• Create—Enables the user to create new objects.• Update—Enables the user to modify existing objects.• Delete—Enables the user to delete existing objects. <p>You can also assign other actions to tenant roles. The other actions include retry, schedule update, schedule delete, activate, reboot, push license, RMA, deploy, schedule, start, disable, deploy, move, run, send, preview, renew, configure, and download.</p>

RELATED DOCUMENTATION

Roles Overview	 42
Role-Based Access Control Overview	 35
About the Tenant Roles Page	 45
Editing, Cloning, and Deleting User-Defined Roles for Tenant Users	 47

Editing, Cloning, and Deleting User-Defined Roles for Tenant Users

IN THIS SECTION

- [Editing Roles](#) | 48
- [Cloning Roles](#) | 48
- [Deleting Roles](#) | 49

You can edit and delete custom (user-defined) roles for tenant users from the Roles page. This topic has the following sections:

NOTE: You cannot modify or delete the predefined roles.

Editing Roles

To modify the parameters configured for a role.

1. Select **Administration > Roles**.

The Roles page appears, displaying the existing role names.

2. Select the role that you want to edit and click the edit icon (pencil) to modify the parameters.

The Edit Role page appears. The fields on the Edit Role page are available for editing.

NOTE: You cannot modify the role name and role scope.

3. Modify the role description and privileges as needed.

4. Click **OK** to save the changes.

A confirmation message appears, indicating the status of the edit operation.

Cloning Roles

You can clone a role (both custom and predefined) when you want to quickly create a copy of an existing role and modify its access privileges.

NOTE: You cannot modify the role name and role scope.

1. Select **Administration > Roles**.

The Roles page appears, displaying the existing role names.

2. Select the role that you want to clone and then click the **Clone** button at the top-right corner of the page.

The Clone Role: *Role-Name* page appears.

3. Specify an appropriate name for the new clone role.

4. Click **OK** to save your changes.

A confirmation message appears, indicating the status of the clone operation.

The name of the clone role is displayed on the Roles page.

5. Select the new clone role and click the edit icon (pencil) to modify its parameters.

The Edit Role page appears.

6. Select the objects, and modify the access privileges of the role, as needed.

7. Click **OK** to save your changes.

A confirmation message appears, indicating the status of the edit operation.

Deleting Roles

To delete a role name:

1. Select **Administration > Roles**.

The Roles page appears, displaying the existing role names.

2. Select the role name that you want to delete and then click the delete icon (X).

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected role name.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

[About the Tenant Roles Page | 45](#)

[Adding User-Defined Roles for Tenant Users | 46](#)

Access Privileges for Role Scopes (Tenant and Operating Company)

This topic describes the access privileges for the tenant and Operating company (OpCo) role scopes. For more information about roles and role scopes, see [“Roles Overview” on page 42](#).

[Table 17 on page 51](#) shows the access privileges for operating company scope.

[Table 18 on page 54](#) shows the access privileges for tenant scope.

Table 17: Access Privileges for Operating Company Scope

Role Scope	Menu Name	Actions	Other Actions
Operating company (OpCo)	Monitor		
	SP Geo Map	Read	-
	Tenants SLA Performance	Read	-
	Alerts	Read and Delete	-
	Alarms	Read	-
	Jobs	Read	Retry Schedule Update Schedule Delete
	Resources		
	POPs	Read, Edit, and Delete	-
	Provider Hub Devices	Read, Edit, and Delete	-
	Tenant Devices	Read	-
	Device Templates	Read, Create, Update, and Delete	Clone Edit Template
	Configuration Templates	Read, Edit, and Delete	-
	Images	Read	-
	Configuration		
	Site management	Edit and Delete	Add provider hub
	Path based steering profiles	Read, Edit, and Delete	-
		Read, Edit, and Delete	-

Table 17: Access Privileges for Operating Company Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	SDWAN Breakout Profiles		
	Application Signatures	Read, Edit, and Delete	-
	Network Services	-	Allocate Server and Detach Server
	Application SLA Profiles	Read, Create, Update, and Delete	-
	Application Traffic Type Profiles	Read	-
	Tenants	Read, Create, Update, and Delete	-
Administration			
	Users	Read, Create, Update, and Delete	-
	Roles	Read, Create, Update, and Delete	-
	Audit Logs	-	Explore and Purge
	Authentication	Read, Create, Update, and Delete	-
	Licenses	Read, Create, Update, and Delete	Push License
	Dynamic Mesh	Edit	-
	Signature Database	Read	Download Signature Database
	SMTP	Read, Create, Update, and Delete	-
	Email Templates	Read and Update	-
	Terms of Use	Update	-
	Display Differences	Modify	-
Help Menu (?)			

Table 17: Access Privileges for Operating Company Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	Getting Started	Read	-
	What's New	Read	-
	Quick Help	Read	-
	Help Center	Read	-
	FAQ	Read	-
	Release Notes	Read	-
	About	Read	-

Table 18: Access Privileges for Tenant Scope

Role Scope	Menu Name	Actions	Other Actions
Tenant	Monitor		
	Tenant GeoMap	Read	-
	Alerts	Read and Delete	Jump to Event Viewer
	Alarms	Read and Delete	
	Link Switch Events	Read	-
	Traffic Logs	Read	View only threat Show exact match Show raw log Create Alert Create Report Export to CSV
	Security Events	Read	Manage Filter Create Alert Create Report
	Application SLA Performance	Read	-
	Application Visibility	Read	-
	User Visibility	Read and Edit	-
	Threats Map (Live)	Read	-
	Jobs	Read	Retry Schedule Update Schedule Delete
	Resources		

Table 18: Access Privileges for Tenant Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	Site Management	Read, Create, and Delete	Configure Upgrade
	Devices	Read and Delete	Activate Push License Reboot RMA Traceroute Ping Configure Stage-2
	Site Groups	Read, Create, Update, and Delete	-
	Mesh Tags	Read, Create, and Delete	-
	Site Templates	Read, Create, Clone, and Delete	-
	Device Templates	Read, Update, and Delete	Import device templates
	Configuration Templates	Read, Update, and Delete	-
	Images	Read	Upgrade History Deploy Stage
	Configuration		
	Firewall Policy	Read, Create, Update, and Delete	Deploy
	Schedule	Read, Create, Update, and Delete	-
	Default Settings	Edit	-
	Unified Threat Management	Read, Create, Update, and Delete	-

Table 18: Access Privileges for Tenant Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	NAT Policies	Read, Create, Update, and Delete	Deploy
	NAT Pools	Read, Create, Update, and Delete	Deploy
	IPS Profiles	Read, Create, Update, and Delete	Clone
	IPS Signatures	Read, Create, Update, and Delete	Clone Clear All Sections
	SSL Proxy Policy	Read, Create, Update, and Delete	Deploy Clone
	SSL Proxy Profiles	Read, Create, Update, and Delete	Clone
	SD-WAN Policy	Read, Create, Update, and Delete	Deploy Clone
	SLA Based Steering Profiles	Read, Create, Update, and Delete	Clone
	Path Based Steering Profiles	Read, Create, Update, and Delete	-
	Cloud Breakout Profiles	Read, Create, Update, and Delete	Assign Sites Detach Sites
	Port Profiles	Read, Create, Update, and Delete	Clone
	Authentication Profiles	Read, Create, Update, and Delete	Clone
	Firewall Filters	Read, Create, Update, and Delete	-
	Access Profiles	Read, Create, Update, and Delete	Clone
	RADIUS Server Profiles	Read, Create, Update, and Delete	Clone
	Address	Read, Create, Update, and Delete	-
	Department	Read, Create, and Delete	-

Table 18: Access Privileges for Tenant Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	Service	Read, Create, Update, and Delete	-
	Application Signature	Read, Create, Update, and Delete	Clone
	Protocols	Read, Create, Update, and Delete	-
	Network Services	Read, Update, and Delete	Start Disable
	Reports		
	Report Definitions - Security	Read, Create, Update, and Delete	Run/Preview Send Clone
	Report Definitions - SD-WAN	Read, Create, Update, and Delete	Run/Preview Send Clone
	Generated Reports -Security	Read and Delete	-
	Generated Reports SD-WAN	Read and Delete	-
	Administration		
	Users	Read, Create, Update, and Delete	-
	Roles	Read, Create, Update, and Delete	-
	Audit Logs		
	Device Licenses	Read, Create, Update, and Delete	Push License
	CSO Licenses	Read	
	Tenant Setting	Read, create, and update	

Table 18: Access Privileges for Tenant Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	Tenant Signature Database	Read	Install
	Certificates	Read, Create, Update, and Delete	-
	Identity Management	Read and Update	-
	Wi-Fi Settings	Read and Update	-
	Help Menu (?)		
	Getting Started	Read	-
	What's New	Read	-
	Quick Help	Read	-
	Help Center	Read	-
	FAQ	Read	-
	Release Notes	Read	-
	About	Read	-

RELATED DOCUMENTATION

[About the Tenant Roles Page | 45](#)
[Role-Based Access Control Overview | 35](#)

SD-WAN and NGFW Deployments

IN THIS CHAPTER

- [SD-WAN and NGFW Workflows for a Tenant Administrator | 59](#)

SD-WAN and NGFW Workflows for a Tenant Administrator

IN THIS SECTION

- [SD-WAN Deployment Workflow | 59](#)
- [NGFW Deployment Workflow | 62](#)

This topic provides information on SD-WAN and Next-Generation Firewall (NGFW) workflows that a Tenant Administrator can perform in the Customer Portal.

NOTE: Before you begin, ensure that your account is activated.

If you're a Tenant Administrator, you can deploy the SD-WAN or NGFW service.

SD-WAN Deployment Workflow

If you deploy the SD-WAN service, CSO intelligently routes traffic through the optimal path based on the criteria you specify in CSO. For example, you can ensure that mission-critical application data is sent over the MPLS link (reliable and secure path) and the non-mission-critical application data is sent over the Internet link (best-effort, non-secure path). CSO also performs load balancing automatically and manages network congestion to route traffic efficiently.

To deploy SD-WAN:

1. Login to the Customer Portal.
2. For SD-WAN, you can add one or more provider hub sites, one or more enterprise hub sites, or a combination of provider hub sites and enterprise hub sites. For SD-WAN Essentials service, you can add only one provider hub site, one enterprise hub site, or a combination of one provider hub site and one enterprise hub site:
 - Add one or more provider hub sites. See [“Add Provider Hub Sites in SD-WAN Deployments” on page 103](#).
 - Add one or more enterprise hub sites. See [“Add Enterprise Hubs with SD-WAN Capability” on page 76](#)

Starting in CSO Release 6.0.0, the ZTP process is simplified to separate the device and service provisioning processes for faster deployment. You can add a site without applying a service and then edit the site to add the SD-WAN service later. See [Add Branch or Enterprise Hub Sites Without Provisioning a Service](#).

NOTE: Starting in CSO Release 6.0.0, adding a hub site is optional for an SD-WAN deployment scenario.

3. If you added enterprise hub sites, perform post-processing tasks for the enterprise hub sites. See *Post-Provisioning Tasks for Enterprise Hub and SD-WAN Spoke Sites*.
4. Add one or more SD-WAN branch sites. See *Add SD-WAN Branch Sites*. To add a site without applying a SD-WAN service, see *Add Branch or Enterprise Hub Sites Without Provisioning a Service*.
5. Perform post-processing tasks for the SD-WAN branch sites. See *Post-Provisioning Tasks for Enterprise Hub and SD-WAN Spoke Sites*.
6. (Optional) Configure a cloud spoke site. [“Adding Cloud Spoke Sites for SD-WAN Deployment” on page 105](#)
7. Monitor SD-WAN sites and devices.

If you want to view	Then visit
General information about the site, WAN overlay and underlay links, policies, and devices	Resources > Site Management > <i>Site-Name</i> For more information, see “Manage a Site” on page 170

If you want to view	Then visit
General information about the device, and view recent alerts and alarms	Resources > Devices > <i>Device-Name</i>. For more information, see “Manage a Single CPE Device” on page 288.
Alerts generated by the SD-WAN CPE or enterprise hub devices	Monitor > Alerts For more information, see “About the Generated Alerts Page” on page 810
Alarms raised by the SD-WAN CPE or enterprise hub devices	Monitor > Alarms For more information, see “About the Alarms Page” on page 817.
SLA performance of the tenant’s sites that have met and not met the defined SLA values	Monitor > Application SLA Performance For more information, see “About the SLA Performance of a Single Tenant Page” on page 856 and “Viewing the SLA Performance of a Site” on page 859.
Applications such as sessions, bandwidth consumed, and risk levels	Monitor > Application Visibility For more information, see “About the Application Visibility Page” on page 866.
Devices (such as top 50 devices accessing high bandwidth-consuming applications and establishing higher number of sessions) on your network	Monitor > User Visibility For more information, see “About the User Visibility Page” on page 869
View the traffic logs from different sites	Monitor > Traffic Logs For more information, see “About the Traffic Logs Page” on page 850
Predefined report definitions or create custom report definitions to generate SD-WAN performance, tenant performance, and site performance reports	Reports > Report Definitions For more information, see “About the SD-WAN Report Definitions Page” on page 906.

NFGW Deployment Workflow

If you deploy the NGFW service at a branch site, you can implement network security at this site using an SRX Series NGFW device as the CPE. You don't need to modify your existing network infrastructure to use the NGFW service. You only need to connect the SRX Series NGFW device to an OAM hub for monitoring and management.

To deploy NGFW service:

1. (Optional) Customize configuration templates. See [“About the Configuration Templates Page” on page 354](#).
2. (Optional) Customize device templates. See [“About the Device Template Page” on page 337](#).
3. Add next-generation firewall site. [“Add a Standalone Next-Generation Firewall Site” on page 153](#).

Starting in CSO Release 6.0.0, the ZTP process is simplified to separate the device and service provisioning processes for faster deployment. You can add a site without applying a service and then edit the site to add the NGFW service later. See *Add Branch or Enterprise Hub Sites Without Provisioning a Service*.
4. Upload and install (push) device licenses. See [“Add a Device License File” on page 403](#) and [“Push a Device License File” on page 405](#).
5. Install the signature database. See [“Manually Installing Signatures” on page 411](#).
6. If you specified that policies should be imported during the activation process, you must deploy the imported policies in CSO:
 - If a firewall policy was imported, deploy the firewall policy.
 - If a NAT policy was imported, deploy the NAT policy.
7. If you did not import the policies as part of the site activation, you can import the policies manually and deploy the policies:
 1. To import firewall policies, go to the Firewall Policy page (Configuration > Firewall > Firewall Policy) and click Import.
 2. To import NAT policies, go to the NAT Policy page (Configuration > NAT > NAT Policy) and click Import.
 3. Deploy the firewall policy and NAT policy.
8. (Optional) Configure unified threat management (UTM) on the next-generation firewall. See [“Creating UTM Profiles” on page 525](#).

9. (Optional) Configure SSL proxy on the next-generation firewall site. See [“Creating SSL Proxy Policy Intents” on page 718](#).
10. (Optional) Configure intrusion prevention system (IPS) on the next-generation firewall. See [“Create IPS Profiles” on page 694](#).
11. Add a firewall policy and zone-based intents and deploy the firewall policy. See [“Adding a Firewall Policy” on page 445](#).
12. (Optional) Add a NAT policy and rules and deploy the NAT policy. See [“Creating NAT Policies” on page 633](#) and [“Deploying NAT Policies” on page 662](#).
13. Monitor the NGFW sites and devices.

If you want to view	Then visit
General information about the site, WAN overlay and underlay links, policies, and devices	Resources > Site Management > <i>Site-Name</i> For more information, see “Manage a Site” on page 170
General information about the device, and view recent alerts and alarms	Resources > Devices > <i>Device-Name</i> . For more information, see “Manage a Single CPE Device” on page 288 .
Alerts generated by the SD-WAN CPE or enterprise hub devices	Monitor > Alerts For more information, see “About the Generated Alerts Page” on page 810
Alarms raised by the SD-WAN CPE or enterprise hub devices	Monitor > Alarms For more information, see “About the Alarms Page” on page 817 .
SLA performance of the tenant’s sites that have met and not met the defined SLA values	Monitor > Application SLA Performance For more information, see “About the SLA Performance of a Single Tenant Page” on page 856 and “Viewing the SLA Performance of a Site” on page 859 .
Applications such as sessions, bandwidth consumed, and risk levels	Monitor > Application Visibility For more information, see “About the Application Visibility Page” on page 866 .

If you want to view	Then visit
Devices (such as top 50 devices accessing high bandwidth-consuming applications and establishing higher number of sessions) on your network	Monitor > User Visibility For more information, see “About the User Visibility Page” on page 869.
View the traffic logs from different sites	Monitor > Traffic Logs For more information, see “About the Traffic Logs Page” on page 850.
Predefined report definitions or create custom report definitions to generate SD-WAN performance, tenant performance, and site performance reports	Reports > Report Definitions For more information, see “About the SD-WAN Report Definitions Page” on page 906.
Traffic logs generated by next-generation firewall devices	Monitoring > Security Events > Traffic Logs. For more information, see “About the Traffic Logs Page” on page 850.
Summary and detailed view of the security events in your network	Monitor > Security Events > All Events For more information, see “About the All Security Events Page” on page 823.
Summary and detailed view of the firewall-related security events	Monitor > Security Events > Firewall. For more information, see “About the Firewall Events Page” on page 828.
Summary and detailed view of the security events related to Web filtering	Monitor > Security Events > Web Filtering For more information, see “About the Web Filtering Events Page” on page 831.
Summary and detailed view of the security events related to IPsec VPNs	Monitor > Security Events > IPsec VPNs For more information, see “About the IPsec VPNs Events Page” on page 834.
Summary and detailed view of the security events related to content filtering	Monitor > Security Events > Content Filtering For more information, see “About the Content Filtering Events Page” on page 836.

If you want to view	Then visit
Summary and detailed view of the security events related to spam	Monitor > Security Events > Antispam For more information, see “About the Antispam Events Page” on page 838.
Summary and detailed view of the security events related to viruses	Monitor > Security Events > Antivirus For more information, see “About the Antivirus Events Page” on page 840.
Summary and detailed view of the security events related to IPS	Monitor > Security Events > IPS For more information, see “About the IPS Events Page” on page 843.
Summary and detailed view screen events that occur as a result of the screen options configured on next-generation firewall devices	Monitor > Security Events > Screen For more information, see “About the Screen Events Page” on page 846.
Incoming and outgoing threats between geographic regions, view blocked and allowed threat events and so on	Monitor > Threat Map (Live) For more information, see “About the Threats Map (Live) Page” on page 875.

2

PART

Managing Sites, Site Groups, and Site Templates

Managing Sites | **67**

Managing Site Groups | **216**

Managing Site Templates | **219**

Managing Mesh Tags | **240**

Managing Dynamic Mesh | **243**

Managing Sites

IN THIS CHAPTER

- About the Site Management Page | 68
- Multihoming Overview | 71
- Enterprise Hubs Overview | 71
- Understand BGP Underlay Routing and Provider Edge (PE) Resiliency | 73
- Upgrading Sites Overview | 75
- Add Enterprise Hubs with SD-WAN Capability | 76
- Add Provider Hub Sites in SD-WAN Deployments | 103
- Adding Cloud Spoke Sites for SD-WAN Deployment | 105
- Provisioning a Cloud Spoke Site in AWS VPC | 115
- Manually Adding Branch Sites | 119
- Add a Branch Site with SD-WAN Capability | 120
- Adding and Provisioning a Next Generation Firewall Overview | 151
- Enabling Integration with Mist Access Points | 152
- Add a Standalone Next-Generation Firewall Site | 153
- Managing LAN Segments on a Tenant Site | 161
- Manage a Site | 170
- Start a Network Service | 178
- Disable a Network Service | 180
- Delete a Network Service | 181
- Add IP VPN Configuration to Provider Hubs | 182
- Edit IP VPN Configuration for Provider Hubs | 185
- Delete IP VPN Configuration from Provider Hubs | 186
- Viewing the Sites History | 187
- Edit Site Overview | 189
- Edit Branch and Enterprise Hub Site Parameters | 192
- Reconfigure Static Tunnels | 203
- Edit Site Examples | 204

● Upgrading Sites | 211

● Delete a Site—Enterprise Hub, Cloud Spoke, and Branch | 213

About the Site Management Page

To access this page, click **Resources > Site Management**.

You can use the **Site Management** page to view and manage existing sites. You can also add different types of sites (manually and by using a site template) and configure the sites with one of the following services:

- Security Services (also referred to as next-generation firewall in this document)
- SD-WAN (Essentials or Advanced) services

Tasks You Can Perform

You can perform the following tasks from this page:

- Add provider hub sites that connect multiple branch sites by establishing IPsec tunnels. See [“Add Provider Hub Sites in SD-WAN Deployments” on page 103](#).
- Add branch sites that represent endpoints at a physical location and connect to hub sites in either a hub-and-spoke or full mesh topology. A branch site can be configured with WAN capabilities.
 - To manually add branch sites, see [“Manually Adding Branch Sites” on page 119](#).
 - To add multiple branch sites by using a site template, see [“Add Branch Sites by Using a Site Template” on page 220](#).
- Add enterprise hub sites that carry site-to-site traffic between branch sites and break out backhaul traffic from the branch sites. See [“Add Enterprise Hubs with SD-WAN Capability” on page 76](#).
- Add cloud branch sites that represent endpoints in a virtual private cloud. See [“Adding Cloud Spoke Sites for SD-WAN Deployment” on page 105](#).
- Add multiple sites by uploading a JSON file. See [“Adding and Configuring Sites by Importing a JSON File” on page 238](#).
- Upgrade one or more sites. See [“Upgrading Sites” on page 211](#).
- Click on the site name to view the site details and to manage the site. See [“Manage a Site” on page 170](#).
- View the jobs executed to add and delete sites for a tenant. see [“Viewing the Sites History” on page 187](#).

- Edit branch and enterprise hub site parameters. See [“Edit Site Overview” on page 189](#).
- Delete a site. See [“Delete a Site—Enterprise Hub, Cloud Spoke, and Branch” on page 213](#).
- View device activation logs. See [“Viewing the History of Tenant Device Activation Logs” on page 257](#).

Field Descriptions

[Table 19 on page 69](#) describes the fields on the **Site Management** page.

Table 19: Fields on the Site Management Page

Field	Description
Alert Icon	<p>Alert associated with the site. The alert can be critical (indicated by a red icon), major (indicated by an orange icon), or minor (indicated by a yellow icon).</p> <p>NOTE: The alert icon is displayed only if there is an alert associated with the site. If there is no alert, no icon is displayed.</p>
Site Name	<p>Name of the tenant site.</p> <p>Click the name of the site to go to the <i>Site-Name</i> page where you can view the site details and configure parameters related to the site. See “Manage a Site” on page 170.</p>
Template	Displays whether a branch site is associated with a site template (displays site template name) or not (-).
Sites Connected To	<p>Number of sites to which the site is connected or N/A (not applicable) if no sites are connected.</p> <p>Mouse over the number to view the list of sites to which the site is connected.</p>
Device Status	Operational status (Up or Down) of the site.
Type	Indicates whether a site is a branch site or a cloud site.
Service	<p>Displays the SD-WAN service level associated with the site.</p> <ul style="list-style-type: none"> • SD-WAN Advanced—Indicates that this site provides the complete SD-WAN service. • SD-WAN Essentials—Indicates that this site provides the basic SD-WAN service.

Table 19: Fields on the Site Management Page (*continued*)

Field	Description
Site Status	<p>The current status of the site:</p> <ul style="list-style-type: none"> • Created—Indicates that the site was added but not configured. • Configured—Indicates that the site was configured but not activated. • Partially-Provisioned—Indicates that one or more DHCP WAN links of the site does not have an IP address after ZTP is complete. The site status changes to Provisioned after an IP address is assigned to the DHCP WAN link. • Provisioned—Indicates that the site is provisioned. • Managed—Indicates that the device is connected to and managed by CSO and is ready for service provisioning. • Upgrade-Required—Indicates that the site needs to be upgraded. • Maintenance—Indicates that the site upgrade is in progress; any deployments that might occur because of other jobs are skipped when the site status is under Maintenance. • Configuration-Failed—Indicates that the deployment of the configuration failed. • Provision-Failed—Indicates that the service provisioning failed.
Local Breakout	Indicates whether local breakout is enabled for at least one WAN link of the site. If it is enabled for at least one WAN link, the number of links on which local breakout is enabled is also displayed. Mouse over the number to view the list of links on which local breakout is enabled.
Version	Contrail Service Orchestration (CSO) version in which the site was added.
Connected Switch(s)	Displays the number of EX Series switches that are connected to the CPE device and are discovered by CSO.
Capabilities	<p>Displays the site capabilities:</p> <ul style="list-style-type: none"> • SD-WAN—Indicates that this site has the SD-WAN Advanced or Essentials service associated with it. • NGFW—Indicates that this site has Security Services capability associated with it.

RELATED DOCUMENTATION

Multihoming Overview

Multihoming is the ability of a branch site to connect to two different hub devices in a hub and spoke topology, thereby providing redundancy. The hub devices function as primary and the secondary hub devices. If there are multiple spokes in the system, the same hub device may act as primary hub device for one spoke and secondary hub device for another spoke. That is, the selection of the primary and the secondary hub devices is only in the context of a branch site. The spoke is connected to both the hub devices through an underlay network.

NOTE: Sites with SD-WAN Essentials service do not support multihoming.

The hub devices can be SRX1500 or SRX4000 series routers. To enable multihoming for a site, you must select the hub and spoke topology when you create the tenant. If you enable multihoming for a site, you must specify a primary and back up site when you configure the site.

Traffic is switched from the primary hub to the secondary hub in the following scenarios:

- The primary hub is down
- The primary hub is up, but all the overlay tunnels between the spoke and the primary hub are down
- The tunnels are up, but the iBGP session between the primary hub and vRR is down. In this case, the failover occurs only after the BGP hold-time expires and the default route is withdrawn.

NOTE: In addition to hub-level redundancy, you can provide VRR-level redundancy by creating two VRRs—primary and secondary—in two different redundancy groups.

Enterprise Hubs Overview

IN THIS SECTION

- [Benefits of Enterprise Hubs](#) | 72

An *enterprise hub* is an SD-WAN site that is used to carry site-to-site traffic between branch sites and to break out backhaul (central breakout) traffic from branch sites. An enterprise hub typically has a data

center department behind it; however, this is not enforced in Contrail Service Orchestration (CSO). You add a enterprise hub from the **Sites** page.

You can add one or more enterprise hubs to act as central breakout (backhaul) nodes and then associate enterprise hubs with branch sites. The enterprise hub that is associated with a spoke site functions like a data hub and performs the following functions:

- Before the creation of site-to-site tunnels, site-to-site traffic to or from a spoke site is sent through the enterprise hub. This traffic triggers the creation of the site-to-site tunnel based on dynamic mesh thresholds and matching mesh tags that you configure for the spoke site.
- If Internet-bound traffic from the spoke site (and all departments associated with the spoke site) is destined for central breakout (backhaul), the traffic first reaches the assigned enterprise hub and then breaks out from the enterprise hub.
- If a provider hub is associated with the spoke site, the provider hub works as a fallback option in case traffic cannot be sent through the enterprise hub.

NOTE: You must attach a branch site (with SDWAN capability) to a provider hub site or an enterprise hub site, or to both hub sites.

If a tenant has more than one enterprise hub configured, CSO statically meshes these sites with overlay tunnels so that the enterprise hubs can exchange routing information for the branch sites with which they are associated. This enables the site-to-site communication between the spoke sites that are associated with different enterprise hubs.

The creation of static tunnels between one enterprise hub and another and between a enterprise hub and a spoke site depends on matching mesh tags. These static tunnels are created during the Zero Touch Provisioning (ZTP) workflow. For more information about mesh tags, see [“Mesh Tags Overview” on page 240](#).

Enterprise hubs can have their own departments similar to other sites. If an enterprise hub does not have directly connected LAN segments in the departments used by the associated spoke sites, then CSO automatically pushes the appropriate department virtual routing and forwarding (VRF) instances to the enterprise hub for connectivity.

Benefits of Enterprise Hubs

- Because enterprise hubs can be used to carry backhaul (central breakout) traffic and are used as an anchor for site-to-site traffic, the volume of traffic sent to the provider hub (controlled by the service provider) is reduced.

RELATED DOCUMENTATION

Understand BGP Underlay Routing and Provider Edge (PE) Resiliency

IN THIS SECTION

- [BGP Underlay Routing and Route Advertisements | 74](#)
- [Benefits of BGP Underlay Routing and PE Resiliency | 74](#)

In Contrail Service Orchestration (CSO), when you add an enterprise hub site or an SD-WAN branch site and enable local breakout on a WAN link, you can enable BGP routing on the underlay network. In addition, you can enable provider edge (PE) resiliency on the underlay network, by specifying primary and secondary PE nodes for a WAN link.

When PE resiliency is enabled for a WAN link, CSO uses the BGP path attribute (local-preference) to give preference to the routes learned from the primary PE node over the routes learned from the secondary PE node. For the PEs to decide the path preference, the as-path-prepend parameter is configured and advertised to the secondary PE to decrement the preference for the secondary BGP route. If the CPE detects that the primary PE node is down, the secondary PE node is used as the route next hop. When the primary node comes back up, the route next hops are changed back to the primary node.

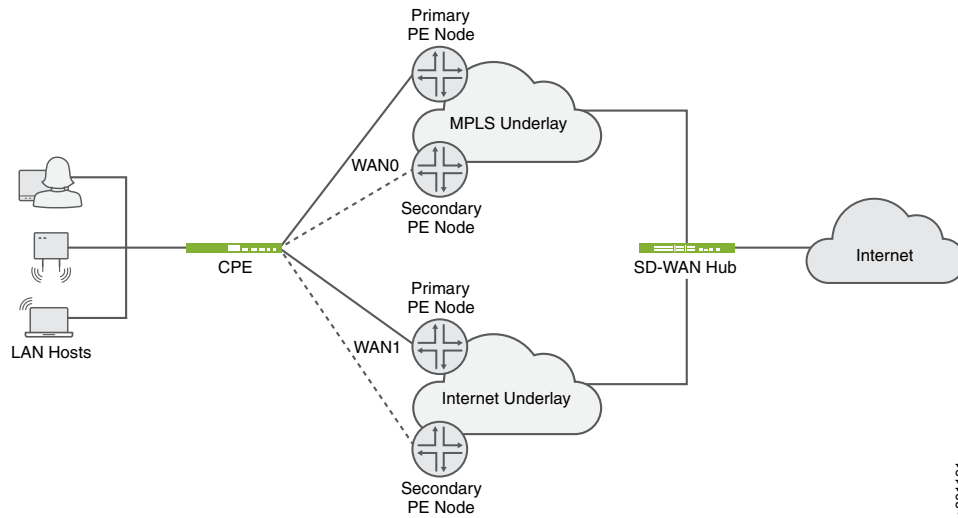
NOTE: To enable BGP underlay routing, you must enable local breakout on the WAN link. However, for traffic to break out locally on the WAN link, you must configure a breakout profile, reference the breakout profile in an SD-WAN policy intent, and deploy the SD-WAN policy.

When you enable BGP underlay routing, CSO installs the routes advertised by the PE nodes on the customer premises equipment (CPE) device. However, CSO does not generate the static default route. Route advertisements to the primary PE node and, if configured, the secondary PE node occur as follows:

- CSO advertises the WAN interface subnet.
- If pool-based translation is configured, CSO advertises the NAT address pool.

[Figure 2 on page 74](#) shows an example of BGP PE resiliency. The CPE device has two WAN links (WAN0 and WAN1); each WAN link is connected to two PE nodes. CSO establishes a BGP peering relationship between the CPE device and the PE nodes connected to the WAN links. CSO allocates BGP attributes in such a way that one PE node acts as the primary node and the other PE node acts as the secondary node.

Figure 2: BGP PE (Provider Edge) Resiliency



BGP Underlay Routing and Route Advertisements

CSO also allows you to advertise public LAN prefixes to the BGP underlay.

NOTE: If a tenant has a public IP address pool configured (in the Tenant-Owned Public IP Pool field during tenant addition) and you enable the advertisement of public LAN prefixes, then for LAN segments that are created with a subnet that falls under the tenant public IP address pool, CSO advertises the LAN subnet to the BGP underlay.

When you enable BGP underlay routing, you can specify the autonomous system (AS) number for the external (EBGP) peer. If the peer AS number is not specified, or if the AS number that is specified is same as the AS number for the site, then the BGP type is assumed to be internal BGP (IBGP). If the specified peer AS number is different from AS number of the site, then the BGP type is assumed to be EBGP.

CSO also provides an option to authenticate BGP routes by using MD5 authentication. When you enable authentication, which is disabled by default, you must specify an authentication key, which is used to verify the authenticity of BGP packets. You must ensure that the BGP peers are also configured with the same MD5 authentication key.

Benefits of BGP Underlay Routing and PE Resiliency

- Public LAN routes can now be advertised to legacy sites, which provides connectivity from SD-WAN sites to legacy sites.

- Previously, there was no capability to exchange underlay prefixes, which meant that users had to configure static routes. With BGP underlay routing, routes are learned dynamically.

RELATED DOCUMENTATION

[Add Enterprise Hubs with SD-WAN Capability | 76](#)

[Add a Branch Site with SD-WAN Capability | 120](#)

Upgrading Sites Overview

When you upgrade Contrail Service Orchestration (CSO), the existing sites continue to have the functionality of earlier releases. However, there might be changes in:

- Device templates
- Image version of a device
- Application configurations (For example, SD-WAN policies)
- Stage-1 and Stage-2 configurations of a device

For CSO to support the latest features in sites that were created in earlier releases, you must upgrade the existing sites to the new version. You can upgrade a single site or upgrade multiple sites simultaneously. When you upgrade multiple sites, ensure that Site Status column of the selected sites displays **Provisioned**.

Users with Tenant Administrators can upgrade a site from the Site Management page. The Site Management page provides information about sites that must be upgraded and sites for which the upgrade is optional.

NOTE: Tenant Administrators cannot upgrade Provider Hub Sites listed in **Site Management** page of the Customer Portal.

In the Site Management page, the following two new columns have been added to indicate whether a site upgrade is mandatory or optional:

- **Site Status**—Indicates the status of the site. If the site status is Provisioned, the upgrade is optional. If the site status is UPGRADE-REQUIRED, the site upgrade is mandatory. You cannot upgrade a site if the site status is Created, Provision Failed, Configured, and Activation Failed.
- **Version**—Indicates the CSO release number in which the site was created.

If you create a site in a release that is tagged as a Long Term Support (LTS) release, the site remains functional in the subsequent two LTS releases. For example, if you have created a site in Release X.2 (LTS release), upgrading the site in Release (X+1).2 and Release (X+2).2 is optional, while it is mandatory to upgrade the site in Release (X+3).2.

If you have created a site in a non-LTS release, the site remains functional in the successive release only. For example if you have created a site in Release X.0 (non-LTS), upgrading the site in Release X.1 is optional, while it is mandatory to upgrade the site in Release X.2.

RELATED DOCUMENTATION

[Upgrading Sites](#) | 211

Add Enterprise Hubs with SD-WAN Capability

An enterprise hub site is an SD-WAN site that is used to carry site-to-site traffic between on-premise spoke sites (branch sites) and to break out backhaul (central breakout) traffic from branch sites. An enterprise hub *typically* has a data center department behind it; however, this is not enforced in Contrail Service Orchestration (CSO). The following device templates are supported for enterprise hubs:

- SRX as SD-WAN CPE (vSRX only)
- Dual SRX as SD-WAN CPEs (vSRX only)
- SRX-1500 as SD-WAN CPE
- Dual SRX1500 as SD-WAN CPEs
- SRX4x00 as SD-WAN CPE
- Dual SRX4x00 as SD-WAN CPEs

NOTE: Starting in CSO Release 6.0.0, in SD-WAN deployments, using hubs to connect sites is optional.

In SD-WAN deployments comprising single or dual customer premises equipment (CPE), tenant administrators have an option to enter the serial number of the CPE device(s) after adding the enterprise hub sites. The enterprise hub can be added by a tenant administrator and activated manually by another authorized user. The authorized user must enter either the serial number and the activation code, or only the serial number when manually activating the device later.

NOTE: In Dual CPE device templates, you cannot add serial number for one CPE and skip entering serial number for the other CPE device. You can either enter serial numbers for both primary and secondary devices while creating the site or enter both serial numbers while activating the site.

Starting in Release 6.0.0, CSO supports the following SD-WAN services for a site:

- *Secure SD-WAN Essentials*—Provides the basic SD-WAN services, ideal for small enterprises. See [“Add a Branch Site with SD-WAN Capability” on page 120](#) for details.

NOTE: A tenant with the Advanced SD-WAN service level can create enterprise hubs only with the Advanced SD-WAN service. A Secure SD-WAN Advanced branch site connects only to secure SD-WAN Advanced enterprise hubs.

- *Secure SD-WAN Advanced*—Provides the complete SD-WAN service. All sites of the tenant with Secure SD-WAN Advanced service are connected in full mesh or hub-and-spoke topology.

NOTE: The SD-WAN sites on CSO Release 5.4 or earlier versions are treated as SD-WAN Advanced sites.

Starting from CSO Release 6.0.0, the enterprise hub site creation workflow is simplified by making the provisioning of services optional during the onboarding process. You can configure the service during the site creation or add the service later. To add an enterprise site without the SD-WAN service, see *Add Branch or Enterprise Hub Sites Without Provisioning a Service*.

To add an enterprise hub site:

NOTE: You can add enterprise hub sites only for tenants with real-time optimized SD-WAN mode.

1. Click **Resources > Site Management**.

The Sites page appears.

2. Click **Add** and select **Enterprise Hub**.

The **Add Enterprise Hub** page appears.

3. Complete configuration settings according to guidelines provided in [Table 20 on page 79](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. (Optional) You can review the configuration in the **Summary** tab and modify the settings, if required.

5. Click **OK**.

- If you entered a serial number during activation and automatic activation is enabled, the Site Activation Progress page appears. The site activation process proceeds through the tasks explained in *Troubleshooting Site Activation Issues*.

Click **OK** to close the Site Activation Progress page.

- If you did not enter a serial number and the automatic activation is disabled, you are returned to the Site Management page. CSO triggers a job and displays a confirmation message with a job link. Click the link to view the status of the job. After the job is finished, CSO displays a confirmation message with a job link. The status of the site changes to **CREATED**.

You must manually activate the device to finish the activation process.

NOTE: The following procedure is applicable if zero touch provisioning (ZTP) is set true in the device template. If ZTP is disabled in the device template, you must copy the stage-1 configuration and commit it on the device for CSO to proceed with the activation.

To manually activate the CPE (enterprise hub) device:

- a. Select the enterprise hub that has to be activated.
- b. Click **Activate Site** link in the Site Management page.

The **Activate Site** page appears.

- c. Enter the serial number(s) of the device and the activation code. Click **OK**.

The **Site Activation Progress** page appears displaying the progress of steps executed for activating the enterprise hub. On successful activation of the device, the Site Status changes from **Created** to **Provisioned**.

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability)

Field	Description
General	
<i>Site Information</i>	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters.
Device Host Name	The device host name is auto-generated and uses the format <i>tenant-name.host-name</i> . You cannot change the <i>tenant-name</i> part in the device host name. Use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.
Site Group	Select a site group to which you want to assign the site.
Site Capabilities	<p>NOTE: Device Management, enabled by default, allows you to create a site with only device management capability (without any services) and add services later.</p> <p>To add an SD-WAN capability for this site, choose one of the following SD-WAN service types:</p> <ul style="list-style-type: none"> Secure SD-WAN Essentials—(Available for tenants with SD-WAN Essentials service level) Provides basic SD-WAN services. This service is ideal for small enterprises looking for managing simple WAN connectivity with comprehensive NGFW security services at the branch sites, using link-based application steering. The SD-WAN Essentials service does not support multihoming, dynamic mesh tunnels, cloud breakout profiles, SLA-based steering profiles, pool based source NAT rules, IPv6, MAP-E, or underlay BGP. Secure SD-WAN Advanced—(Available for tenants with SD-WAN Advanced service level) Provides complete SD-WAN services. This service is ideal for enterprises with one or more data centers, requiring flexible topologies and dynamic application steering. You can establish site-to-site connectivity by using a hub in a hub-and-spoke topology or through static or dynamic full mesh VPN tunnels. Enterprise wide intent based SD-WAN policies and service-level agreement (SLA) measurements allow to differentiate and dynamically route traffic for different applications. <p>NOTE: A Secure SD-WAN Advanced branch site connects only to secure SD-WAN Advanced enterprise hubs.</p>
<i>Address and Contact Information</i>	
Street Address	Enter the street address of the site.

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
City	Enter the name of the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	<p>Select the country where the site is located.</p> <p>You can click the Validate button to verify the address that you specified:</p> <ul style="list-style-type: none"> • The Site address verification successful message is displayed if the address can be verified. You can click the View location on a map link to see the address location. • If the address cannot be verified, the Site address could not be validated message is displayed .
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	<p>Enter the phone number of the contact person for the site.</p> <p>Click Next to continue.</p>
<i>Advanced Configuration</i>	
Domain Name Server	<p>Specify one or more IPv4 or IPv6, or both IPv4 and IPv6 addresses of the DNS server. To specify more than one DNS server address, type the address, press Enter, and then type the next address, and so on.</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
Device	
NOTE: Some fields in this section are displayed only if you enable the Device Redundancy option.	

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Device Redundancy	<p>Disabled by default. Enable this option for dual CPEs.</p> <p>The following prerequisites are necessary for enabling device redundancy:</p> <ul style="list-style-type: none"> • Ensure that the control and fabric ports between both the nodes are connected. • Ensure that the device is preconfigured for management connectivity (factory-default or prestaged). Do not configure the control, fabric, and data (reth) ports as these ports will be reconfigured. <p>To identify the control, fabric, management, and data ports for each SRX model, refer to the SRX High Availability Configurator tool.</p> <p>NOTE: Do not generate the configuration in the tool as CSO generates and applies the cluster configuration automatically.</p> <ul style="list-style-type: none"> • If you are using ZTP on SRX300 and SRX320 devices, use ge-0/0/7 as the predefined DHCP port instead of ge-0/0/0. • Provide the fabric and data (reth) port information in the device template. The control and fxp0 ports are predefined. To change the control port, change it in the platform device template. To change the data (reth) port, change it in the SDWAN device template.
Device Series	<p>Select the device series to which the CPE belongs.</p> <p>Based on the device series that you select, the supported device templates (containing information for configuring devices) are listed.</p>
Device Model	Select the device model number.
Device Root Password	The default root password is fetched from the ENC_ROOT_PASSWORD field in the device template. You can retain the password or change it by entering a password in plain-text format. The password is encrypted and stored on the device.
Serial Number	<p>For a single CPE device, enter the serial number of the CPE device. Serial numbers are case-sensitive.</p> <p>If you do not enter serial number, the enterprise hub is added but not activated. See “Step-by-Step Procedure” on page 78 to enter serial number and activate the enterprise hub site later.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Node 0 Serial Number	<p>For dual CPEs, enter the serial number of the primary CPE device. The serial number is case sensitive.</p> <p>If you do not enter serial number, the enterprise hub site is added but not activated. See “Step-by-Step Procedure” on page 78 to enter serial number and activate the enterprise hub site later.</p>
Node 1 Serial Number	<p>For dual CPEs, enter the serial number of the secondary CPE device. The serial number is case sensitive.</p> <p>If you do not enter serial number, the enterprise hub site is added but not activated. See “Step-by-Step Procedure” on page 78 to enter serial number and activate the enterprise hub site later.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Zero Touch Provisioning	<p>Click the toggle button to enable or disable Zero Touch Provisioning (ZTP). This option is enabled by default.</p> <p>To use ZTP, ensure the following:</p> <ul style="list-style-type: none"> Device must have connectivity to CSO and Juniper phone-home server (https://redirect.juniper.net) <p>Use telnet to verify connectivity:</p> <pre>telnet redirect.juniper.net:443 telnet CSO Hostname/IP:443</pre> <p>If the connection is established, the device has connectivity to the phone-home server and CSO.</p> <ul style="list-style-type: none"> Required certificates for phone-home server and CSO must be present on the device. <p>If you enable ZTP, the Boot Image field is displayed and you must select an image that supports the Phone-Home client. During ZTP, the image on the firewall device is upgraded to the image that you select for the Boot Image.</p> <p>If you disable ZTP, ensure that the device has connectivity to CSO. If the device is not prestaged or preconfigured, then you must provide the details under the Management Connectivity section so that CSO can generate the configuration as part of the stage-1 configuration. You can skip the Management Connectivity section if the device has connectivity to CSO.</p> <p>If you disable ZTP, you must copy the stage-1 configuration from CSO and commit it on the device to start the onboarding process. Use any of the following options to copy the stage-1 configuration:</p> <ul style="list-style-type: none"> Click the Click to copy stage-1 config link next to Prestage Device task on the Site Activation Progress page. <p>If you close the Site Activation Progress page inadvertently, you can access the page from the Site Management page. Click the View link next to the status of the site under the Site Status column.</p> <ul style="list-style-type: none"> On the Devices page (Resources > Devices), select the device and click Stage1 Config.
Is Cluster Already Formed?	<p>NOTE: This field is available only for SRX dual CPE devices.</p> <p>Click the toggle button to specify whether the SRX cluster has been manually formed (Yes) or not (No).</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Cluster ID	<p>NOTE: This field is available only for SRX dual CPE devices.</p> <p>If the SRX cluster hasn't been formed manually, specify a unique ID for the cluster.</p> <p>Range: 1 through 15</p> <p>If you've enabled ZTP for the site, the cluster is automatically formed when the site is activated. If you've disabled ZTP, the following processes are displayed on the Site Activation Progress page (that appears after you've added the branch site):</p> <ol style="list-style-type: none"> 1. After CSO models the site (that is, after the Model Site process completes successfully), click the Click to copy pre script link, which appears next to the Pre Script process. 2. Execute the commands as directed. <p>After the Pre Script process completes successfully, the SRX cluster is formed and the recovery.conf file is saved on the cluster. In case you want to delete the site later, you'll need this file to remove the stage-1 configuration and other configurations pushed to the device by CSO.</p> 3. Manually copy the stage-1 configuration (generated automatically by CSO) to the primary device in the cluster and commit the configuration on the device. <p>After the cluster is detected, CSO executes the bootstrap and provisioning processes and completes provisioning the cluster.</p>
Auto Activate	Click the toggle button to enable (default) or disable automatic activation of the CPE device.
Activation Code	If the automatic activation of the device is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.
Node 0 Activation Code	If the automatic activation of dual CPEs is disabled, enter the activation code to manually activate the primary CPE device.
Node 1 Activation Code	If the automatic activation of dual CPEs is disabled, enter the activation code to manually activate the secondary CPE device.

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Management Interface Family	Select the IP address type (IPv4 or IPv6) for the management interface. This field is displayed only if you have enabled Zero Touch Provisioning .
Boot image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the CPE device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image is populated based on the device template that you have selected while creating a site. See <i>Uploading a Device Image</i>.</p>
(Device Template)	Select a device template, which contains information for configuring a device.
Management Connectivity	
<p>NOTE: This section is displayed only when Zero Touch Provisioning is disabled. If you are adding a chassis cluster, then you must provide the interface details for both the nodes.</p>	
Address Family	Select the IP address type (IPv4 or IPv6).
Interface Name	This is the WAN interface that the device uses to connect to CSO.
Access Type	Select the access type for the underlay link. LTE, ADSL, and VDSL access types are supported only on Internet links. You cannot add LTE, ADSL, and VDSL access types to the same WAN link.
Address Assignment	DHCP is selected by default. If you want to provide a static IP address, select STATIC.
Management VLAN ID	<p>Enter a VLAN ID for the WAN link.</p> <p>Range: 0 through 4094</p>
PPPoE	Click the toggle button to enable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet).

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
<i>Hub Configuration</i>	
<p>NOTE: Hub selection is optional for both SD-WAN Advanced and Essentials sites. SD-WAN Essentials sites do not support multihoming. However, you can edit an Essentials site (post activation) to upgrade it to an Advanced site and add a secondary hub later if required, provided that the tenant's service level is upgraded to Advanced.</p>	
Primary Provider Hub	<p>Select the provider hub site (or primary provider hub site in case of multihoming) to which you want to connect the enterprise hub site.</p> <p>If you do not specify a provider hub site, then the enterprise hub site can connect only to the branch sites that are associated with the enterprise hub site.</p> <p>If you specify a provider hub site, then the enterprise hub site can also connect to the branch sites to which that provider hub site is associated.</p>
Secondary Provider Hub	<p>NOTE: Not applicable to sites with SD-WAN Essentials service.</p> <p>Select the secondary provider hub site (in case of multihoming) to which you want to connect the enterprise hub site.</p> <p>When the primary provider hub is down, the enterprise hub connects to the secondary provider hub and the branch sites to which that provider hub site is associated.</p>
<i>WAN Links</i>	
<p>NOTE: In Release 6.1.0, CSO moves a site to the PROVISIONED state when at least one of the WAN links obtains the IP address and is activated. You can activate the remaining DHCP WAN links later. If the provisioned site establishes Dynamic VPN (DVPN) tunnels to other sites before the DHCP WAN links are activated, then these DHCP WAN links participate in DVPN only when the tunnels are deleted and added back (that is, traffic between a pair of sites falls below the delete threshold, and then crosses the create threshold again).</p>	
WAN_0 (WAN-Interface-Name)	<p>This field is enabled by default.</p> <p>Enter parameters related to the WAN_0 (WAN-Interface-Name) link. Fields marked with an asterisk (*) must be configured to proceed.</p>
Link Type	Select whether the link would be an MPLS link or Internet link.
Egress Bandwidth	<p>Enter the maximum bandwidth (in Mbps) that the CPE allows towards the WAN link.</p> <p>Range: 1 through 10,000.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Public IP Address	<p>Enter the public IPv4 address for the link.</p> <p>NOTE: This IP address should be provided only if the static IP prefix is a private IP address and 1:1 NAT is configured.</p>
<i>Underlay Address Families</i>	
IPv4	<p>By default, IPv4 address assignment is enabled for the WAN link.</p> <p>The WAN link requires an IPv4 address to connect to an IPv4 network.</p>
Address Assignment Method	<p>Displays the method of assigning an IPv4 address to the WAN link (STATIC). You cannot modify this field.</p> <p>You must provide the IPv4 address prefix and the gateway IPv4 address for the WAN link.</p>
Static IP Prefix	Enter the IPv4 address prefix of the WAN link.
Gateway IP Address	Enter the IPv4 address of the gateway of the WAN service provider.
WAN Link (Primary or Secondary)	For dual CPE device templates, displays whether the WAN link is a primary link or a secondary link. You cannot modify this field.
<i>Advanced Settings</i>	
Address Family (Tunnel Creation)	Displays the underlay address family (IPv4) that is used to establish the overlay tunnel.
Provider	Enter the name of the service provider providing the WAN service.
Cost/Month	<p>Enter the cost for using the WAN link per month and select the currency in which the cost is indicated from the adjacent drop-down list.</p> <p>Range: 1 through 10,000.</p> <p>In bandwidth-optimized SD-WAN, CSO uses this information to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.</p>
Link Priority	<p>Enter a value in the range 1-255. A lower value indicates a more preferred link. A value of 1 indicates highest priority and a value of 255 indicates lowest priority. If you do not enter a value, the link priority is considered as 255.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Enable Local Breakout	<p>Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent. • If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.
Breakout Options	<p>When the Enable Local Breakout field is enabled, select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.</p>
Autocreate Source NAT Rule	<p>NOTE: Sites with Secure SD-WAN Essentials service support interface-based source NAT rules only. If you enable this options for an SD-WAN Essentials site, interface-based source NAT rules are automatically applied. If you enable this options for an SD-WAN Advanced site, you must select a source NAT rule from the Translation field.</p> <p>Click the toggle button to enable or disable the automatic creation of source NAT rules. By default, this field is enabled when local breakout is enabled on the WAN link.</p> <p>Table 21 on page 96 explains how source NAT rules are automatically created on the WAN link. The automatically-created source NAT rules are implicitly defined and applied to the site and is not visible on the NAT Policies page.</p> <p>NOTE: You can manually override automatically created NAT rules, by creating a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant department zone and WAN interface as the source and destination. For example:</p> <pre>Dept-Zone1 --> W1 : Translation=Pool-2</pre> <p>The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.</p> <p>You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:</p> <pre>Dept-Zone1, Port 56578 --> W1: Translation=Pool-2</pre>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Translation	<p>This field is displayed only if the automatic creation of source NAT rules is enabled for the WAN link, and the SD-WAN service used is Advanced. Sites with Secure SD-WAN Essentials service support interface-based source NAT rules only.</p> <p>Select the type of NAT to use for the traffic on the WAN link:</p> <ul style="list-style-type: none"> • Interface—Use interface-based NAT, which is the default. • Pool—Use pool-based NAT. If you select this option, you must specify the IP addresses that are to be used for the NAT pool. <p>NOTE: No NAT is performed for tenant-owned public IP addresses that were added during the tenant addition workflow.</p>
IP Addresses	<p>For pool-based NAT, enter one or more IP addresses, subnets, or an IP address range. Separate multiple IP addresses by using commas and use a hyphen to denote a range; for example, 192.0.2.1-192.0.2.50.</p>
Preferred Breakout Link	<p>Click the toggle button to enable a WAN link as the most preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>
BGP Underlay Options	<p>NOTE: Not applicable to sites with the SD-WAN Essentials service.</p> <p>NOTE: This setting can be configured only if the address assignment is static and local breakout is enabled.</p> <p>Click the toggle button to enable BGP underlay routing.</p> <p>When you enable BGP underlay routing, route advertisements to the primary PE node and, if configured, the secondary PE node occur as follows:</p> <ul style="list-style-type: none"> • CSO advertises the WAN interface subnet. • If you configured pool-based translation, CSO advertises the NAT address pool. <p>NOTE: If underlay BGP is enabled for a WAN link, then the routes learnt from BGP are installed for local breakout; CSO does not generate the static default route.</p>
Primary Neighbor	<p>Displays the IP address that you entered for the gateway for the WAN link.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Secondary Neighbor	<p>If you want to provide PE resiliency, you can configure a secondary PE node.</p> <p>Enter the IP address of the secondary PE node.</p> <p>NOTE: If the primary PE node goes down, then the secondary PE is used as the next hop. When the primary PE comes back up, the route next hops are changed to the primary PE.</p>
eBGP Peer-AS-Number	<p>Enter the autonomous system (AS) number for the external (EBGP) peer.</p> <p>NOTE: If the peer AS number is not configured or the peer AS number that is configured is the same as that of the CPE site, then the BGP type is assumed to be internal BGP (IBGP).</p>
Local AS Number	<p>Enter the local AS number for the WAN link. When you configure this parameter, the local AS number is used for eBGP peering instead of the global AS number configured for the device.</p> <p>NOTE: The local AS number must be different from the global AS and eBGP peer AS numbers.</p>
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> • None—Indicates that no authentication should be used. This is the default. • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.
Auth Key	<p>If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.</p>
Advertise Public LAN Prefixes	<p>Click the toggle button to enable the advertisement of public LAN prefixes. This field is disabled by default.</p> <p>If the tenant has a public IP address pool configured and you enable the advertisement of public LAN prefixes, then for LAN segments that are created with a subnet that falls under the tenant public IP address pool, CSO advertises the LAN subnet to the BGP underlay.</p> <p>NOTE: When public LAN advertisement is enabled for the WAN link, public LAN prefixes are advertised through the BGP underlay towards MPLS or the Internet. If a site has two versions of the route installed for the same LAN prefix in the overlay and underlay, the overlay routes are always preferred over underlay.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Use For Fullmesh	<p>Click the toggle button to specify whether the WAN link can be a part of a full mesh topology.</p> <p>A site can have all WAN links enabled for meshing.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • For link redundancy, you must enable at least two WAN links for full mesh. • Even if you enable this option, sites with SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or a tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.
Mesh Overlay Link Type	<p>When Use for Fullmesh field is enabled, select the type of mesh overlay link—GRE and GRE_IPSEC.</p> <ul style="list-style-type: none"> • If the link type is Internet, the value for mesh overlay link type is GRE_IPSEC. • If the link type is MPLS, select one of the following options: <ul style="list-style-type: none"> • GRE-IPSEC • GRE
Mesh Tag	<p>When the Use for Fullmesh field is enabled, select one or more mesh tags to be associated with the WAN link for creating tunnels.</p> <p>Matching mesh tags is one of the criteria used to form tunnels between sites that support meshing.</p> <p>For more information about mesh tags, see “Mesh Tags Overview” on page 240.</p>
Connects to Provider Hubs	<p>NOTE: The Connects to Provider Hubs field is available only if you have selected a provider hub.</p> <p>Click the toggle button to specify that the WAN link of the site connects to a provider hub.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted. • For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Overlay Tunnel Type	<p>This field is displayed when the Connects to Provider Hubs field is enabled and only one provider hub (primary) is specified.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) for the tunnel to the primary hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device	<p>This field is displayed when the Connects to Provider Hubs field is enabled and only one provider hub (primary) is specified.</p> <p>Displays the peer hub device to which the site is connected.</p>
Overlay Peer Interface	<p>This field is displayed when the Connects to Provider Hubs field is enabled and only one provider hub (primary) is specified.</p> <p>Select the interface name of the hub device to which the WAN link of the site is connected.</p>
Overlay Tunnel Type 1	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) for the tunnel to the primary hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device 1	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Displays the primary peer hub device to which the site is connected.</p>
Overlay Peer Interface 1	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the interface name of the primary hub device to which the WAN link of the site is connected.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Overlay Tunnel Type 2	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) for the tunnel to the secondary hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device 2	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Displays the secondary peer hub device to which the site is connected.</p>
Overlay Peer Interface 2	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the interface name of the secondary hub device to which the WAN link of the site is connected.</p>
Backup Link	<p>Select a backup link through which traffic can be routed when the primary (other) links are unavailable. You can select any link other than the default links or links that are configured exclusively for local breakout traffic.</p> <p>When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. However, SLA data is not monitored for the backup link.</p>
Default Link	<p>Select one or more links that will be used for routing traffic in the absence of matching SD-WAN policy intents. A site can have multiple default links to the hub site.</p> <p>Default links are used primarily for overlay traffic but can also be used for local breakout traffic. However, a default link cannot be used exclusively for local breakout traffic. If you do not specify a default link, then equal-cost multipath (ECMP) is used to choose the link on which to route traffic.</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
VLAN ID	<p>Enter a VLAN ID for the WAN link.</p> <p>Range: 0 through 4049 (4050 to 4094 is reserved by CSO).</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you are configuring more than one WAN link on the same physical interface, only one WAN link can be untagged; for the remaining WAN links, you must configure a VLAN ID. • A combination of tagged and untagged on the same physical interface is supported only for single CPE devices. • You cannot have a combination of tagged and untagged WAN links on the same et interface. If you are configuring multiple WAN links on the same et interface, then you must specify a VLAN ID for all the links. <p>To enable the configuration of WAN links as logical interfaces in SD-WAN branch sites, the SP Administrator user must modify the device template and configure the WAN ports as logical interfaces.</p>
WAN_1 (WAN-Interface-Name)	<p>Click the toggle button to enable or disable (default) the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed.</p> <p>Refer to the fields described for WAN_0 (WAN-Interface-Name) for an explanation of the fields</p>
WAN_2 (WAN-Interface-Name)	<p>Click the toggle button to enable or disable (default) the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed.</p> <p>Refer to the fields described for WAN_0 (WAN-Interface-Name) for an explanation of the fields</p>
WAN_3 (WAN-Interface-Name)	<p>Click the toggle button to enable or disable (default) the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed.</p> <p>Refer to the fields described for WAN_0 (WAN-Interface-Name) for an explanation of the fields</p>

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
<i>Advanced Configuration</i>	
<p>NOTE: Sites with Secure SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or a tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.</p>	
OAM IP Prefix	<p>Enter an IPv4 address prefix (such as 10.100.100.11/32) for the loopback interface on the CPE device. The IP address prefix should be a /32 IP address prefix and must be unique across the entire management network.</p> <p>NOTE: We recommend that you do not configure this setting (leave the IP Prefix field blank) because management connectivity is handled automatically by CSO.</p>
DVPN Threshold for Tunnel Creation	<p>NOTE: Not applicable to sites with SD-WAN Essentials service.</p> <p>Specify the threshold for the number of sessions (flows) closed (in a two-minute duration) between the enterprise hub and a destination site. When the number of sessions closed exceeds the specified threshold, a tunnel is created between the enterprise hub and the destination site.</p> <p>The default value is 5.</p> <p>For example, if you specify the Create Threshold as 5, dynamic mesh tunnels are created if the number of sessions closed between the enterprise hub and destination site exceeds 5 in 2 minutes.</p>
DVPN Threshold for Tunnel Deletion	<p>NOTE: Not applicable to sites with SD-WAN Essentials service.</p> <p>Specify the threshold for the number of sessions closed (in a 15-minute duration) between the enterprise hub and a destination site. When the number of sessions closed is lower than the specified threshold, the tunnel between the enterprise hub and destination site is deleted.</p> <p>The default value is 2.</p> <p>For example, if you specify the number of sessions closed as 2, dynamic mesh tunnels between the enterprise hub and destination site are deleted if the number of sessions closed is lesser than or equal to 2.</p>

LAN Segment Configuration

Refer to [Table 22 on page 98](#) for configuring LAN segments.

Configuration Templates (Optional)

Table 20: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability) (continued)

Field	Description
Configuration Templates List	<p>Select one or more configuration templates from the list. This list is filtered based on the device that you select.</p> <p>Configuration templates are stage-2 templates that are added by your OpCo administrators or SP administrators or Tenant administrators.</p> <p>NOTE: You must set the parameters of the configuration templates that you have selected before you move to the LAN section.</p> <p>To set the parameters for the selected configuration templates:</p> <ol style="list-style-type: none"> 1. After you select one or more configuration templates, click Set Parameters. The Device Configurations page appears. This page consists of two tabs—Configure and Summary 2. In the Configure tab fill in the attributes for each of the configuration templates. (Optional) View the CLI commands in the Summary tab. 3. Click Save. You have added and set the parameters for the configuration templates that are part of the site template that you are creating.

Refer to [Table 22 on page 98](#) for configuring LAN segments.

Table 21: Automatic Creation of Source NAT Rules

Autocreate Source NAT Rule	Translation	NAT Rules Creation
Disabled	Not applicable (No NAT)	None.

Table 21: Automatic Creation of Source NAT Rules (*continued*)

Autocreate Source NAT Rule	Translation	NAT Rules Creation
Enabled	Interface-Based (Default)—CSO creates interface-based NAT rules.	<p>Source NAT rules are automatically created, with each rule from a department zone to the WAN interface, with a translation of type interface. Each pair of [zone - interface] represents a rule-set.</p> <p>For example, the following department zone to (WAN link) W1 interface rule-set might be created:</p> <pre>Dept-Zone1 --> W1: Translation=Interface Dept-Zone2 --> W1: Translation=Interface Dept-Zone3 --> W1: Translation=Interface</pre> <p>When traffic from a branch site breaks out at an enterprise hub, a source NAT rule is automatically created at the enterprise hub from the department routing group (also referred to as VRF group) to the WAN interface.</p> <pre>Dept-vrf-group --> W1: Translation=Interface</pre>
Enabled	Pool-Based—CSO automatically creates pool-based NAT rules (Not applicable to sites with SD-WAN Essentials service).	<p>Source NAT rules are automatically created, with each rule from a department zone to the WAN NAT pool with a translation of type pool.</p> <p>For example, a source NAT rule from department zone to NAT pool might be created:</p> <pre>Dept-Zone1 --> W1 : Translation=Pool-1 Dept-Zone2 --> W1 : Translation=Pool-1</pre> <p>When traffic from a branch site breaks out at an enterprise hub, a source NAT rule is automatically created at the enterprise hub from the department routing group to the WAN pool.</p> <pre>Dept-vrf-group --> W1: Translation=Pool</pre>

Table 22: Add LAN Segment Settings

Field	Description
Use for Overlay VPN	<p>Enable the Use for Overlay VPN field to associate the LAN segment with the selected department (VRF + ZONE) for overlay traffic to other sites.</p> <p>Disable the Use for Overlay VPN field to associate the LAN segment with a security zone for underlay breakout. You must define zone-based security policies.</p> <p>NOTE: When adding a new site, this field is enabled by default and cannot be modified. However, when you add a new LAN Segment to a provisioned site from the LAN tab of the Site-Name page, you can enable or disable this option.</p>
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length allowed is 15 characters.</p>
CPE Port	<p>NOTE: Applicable to SRX Series devices.</p> <p>Select the CPE port to be added in the LAN segment.</p> <p>When you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page, you can select (or create) a LAG interface or a redundant Ethernet (reth) interface (for dual CPE cluster) to connect the SRX Series CPE devices to an EX series switch.</p> <p>To use the et interface on SRX4600 devices, you must create a LAG interface and configure the et interface as a member of the LAG (aggregated Ethernet or ae) interface. See “Create LAG Interface” on page 312.</p> <p>For an SRX4600 dual CPE cluster, you can use the et interface if it is configured as a member of the redundant Ethernet (reth) interface.</p>
Add LAG Interface	<p>NOTE: This option is available when you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page.</p> <p>Click the link to create a LAG interface (ae interface) if you want to use it to connect the SRX Series CPE to the EX Series switch. See “Create LAG Interface” on page 312 for details.</p>
Create RETH Interface	<p>NOTE: This option is available when you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page.</p> <p>Click the link to create a reth interface for an SD-WAN site with a dual CPE cluster. See “Create a RETH Interface” on page 314 for details.</p>

Table 22: Add LAN Segment Settings (*continued*)

Field	Description
Type NOTE: This field is displayed only for LAN segments associated with enterprise hub sites.	Select the type of LAN segment: <ul style="list-style-type: none"> • Directly Connected (default)—Indicates that the LAN segment is directly connected to the site. • Dynamic Routed—Indicates that the LAN segment is not directly connected to the site and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.
VLAN ID	Enter the VLAN ID for the LAN segment. By default, VLAN ID is set to 1 and native VLAN is enabled for untagged traffic. Range: 1 to 4049 .
Use for Native VLAN	Enable this option to use the VLAN ID specified above for untagged traffic. The CPE interface is configured with a native-vlan-id, which has the same value as the VLAN ID.
Department	NOTE: This field is available only if the Use for Overlay VPN field is enabled. Select a department to which the LAN segment is assigned. Alternatively, click the Create Department link to create a new department and assign the LAN segment to it. See “Add a Department” on page 783 for details. You can group LAN segments as departments for ease of management and for applying policies at the department-level. For LAN segments that are dynamically routed, you can assign only a data center department.
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment. This address will be the default gateway for endpoints in this LAN segment. For example: 192.0.2.8/24.
Zone	NOTE: This field is available only if the Use for Overlay VPN field is disabled. Select a security zone to be associated with this LAN segment. Alternatively click Create Zone to create a new security zone and assign that to this LAN segment. See “Adding a Security Zone” on page 318 for details.
DHCP	For directly connected LAN segments, click the toggle button to enable DHCP. You can enable DHCP if you want to assign IP addresses by using a DHCP server or disable DHCP if you want to assign a static IP address to the LAN segment. NOTE: If you enable DHCP, additional fields appear on the page.

Table 22: Add LAN Segment Settings (*continued*)

Field	Description
Additional fields related to DHCP	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server. Default: 1440 Range: 0 through 4,294,967,295 seconds.
Name Server	Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address. NOTE: DNS servers are used to resolve hostnames into IP addresses.
CPE Ports	NOTE: Applicable to NFX150 and NFX250 devices. For sites with SD-WAN capability, the CPE Ports field is disabled and the CPE ports that you can include in the LAN segment are listed. Select the ports from the Available column and click the right-arrow to move the ports to the Selected column.
Static Routing	
Use this section to configure static routing on the LAN segment. Provide the IP addresses of all the LAN routers connected to the CPE device and the static subnets behind these routers.	
<i>Add LAN Router IP Prefix</i>	
LAN Router IP	Enter the IP address of the LAN router that is connected to the CPE device.
Prefix	Enter the subnets that are connected to the LAN router.
BFD	Enable Bidirectional Forwarding Detection (BFD) to detect any failures on the static route.

Table 22: Add LAN Segment Settings (*continued*)

Field	Description
<i>Dynamic Routing</i>	
Routing Protocol	Enable this toggle button to configure dynamic routing using the BGP or OSPF protocol.
BFD	Enable Bidirectional Forwarding Detection (BFD) to detect any failures in the LAN segment.
Protocol	Select either BGP or OSPF.
<p>BGP Configuration</p> <p>NOTE: Starting in Release 6.1.0, CSO explicitly disables the long-lived graceful restart (LLGR) capability for BGP peering sessions with provider edge (PE) and data center or LAN routers. Disabling LLGR ensures that the CPE does not differentiate the route advertisements to the peering router irrespective of the peering router's LLGR capability.</p> <p>Prior to CSO Release 6.1.0, LLGR helper mode is enabled by default (implicit behavior of Junos OS) on the CPE for BGP peering towards PE router in IP VPN deployments, and data center or LAN routers in data center deployments.</p>	
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> • None—Indicates that no authentication should be used. This is the default. • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.
BGP Options	<p>You can select the following options based on your requirements:</p> <ul style="list-style-type: none"> • AS-OVERRIDE: Replaces all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer. • AS-PATH-PREPEND: Prepends one or more autonomous system (AS) numbers at the beginning of an AS path. Prepending an AS path makes a shorter AS path look longer and therefore it becomes less preferable to BGP. • AS-LOOP: Allows the local device's AS number to be added in the received AS paths. You can specify the number of times the detection of local AS is allowed in the AS path.
Loop Count	<p>This field is displayed only if you select AS-LOOP.</p> <p>Enter the maximum number of times the detection of local AS is allowed in the AS path.</p>

Table 22: Add LAN Segment Settings (*continued*)

Field	Description
Peer IP Address	Enter the IP address of the LAN BGP peer.
Peer AS Number	Enter the autonomous system (AS) number of the LAN BGP peer. By default, CSO uses the AS number 64512. You can enter a different AS number.
Local AS Number	Enter the local AS number. When you configure this parameter, the local AS number is used for BGP peering instead of the global AS number configured for the CPE.
<i>OSPF Configuration</i>	
OSPF Area ID	Specify the OSPF area identifier to be used for the dynamic route.
Authentication	<p>Select the OSPF route authentication method to be used:</p> <ul style="list-style-type: none"> • Password—Indicates that password-based authentication should be used. If you choose this option, you must specify the password. (This is the default). • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key. • None—Indicates that no authentication should be used.
Password	Enter the password to be used to verify the authenticity of OSPF packets.
Confirm Password	Retype the password for confirmation purposes.
MD5 Auth Key ID	<p>If you specified that MD5 should be used for authentication, enter the OSPF MD5 authentication key ID.</p> <p>Range: 1 through 255.</p>
Auth Key	If you specified that MD5 should be used for authentication, enter an MD5 authentication key, which is used to verify the authenticity of OSPF packets.
<i>Route Advertisement Control</i>	
LAN Route(s) to Overlay	When this option is enabled, LAN routes are advertised to the remote CPEs. By default, this option is enabled.

Table 22: Add LAN Segment Settings (*continued*)

Field	Description
Overlay Route(s) to LAN	<p>This option is displayed only if you enable the Routing Protocol toggle button. By default, this option is disabled.</p> <p>Enable this option to advertise the remote CPE routes received in a department to the LAN router.</p> <p>NOTE: In CSO Release 6.0.0 and earlier releases, this option is called Advertise LAN Prefix and is applicable only for data center departments.</p>
Static/Aggr Routes to Overlay	<p>Enable this option to allow advertisement of static or aggregate routes to the overlay network.</p> <ul style="list-style-type: none"> • If a large number of LAN routes are present, then you can disable the LAN Route(s) to Overlay option and use this option to advertise aggregate routes. • If you want to advertise additional routes, then you can enable the LAN Route(s) to Overlay option and use this option to advertise additional static routes.

RELATED DOCUMENTATION

[About the Site Management Page | 68](#)
[Enterprise Hubs Overview | 71](#)

Add Provider Hub Sites in SD-WAN Deployments

Provider hub sites are logical entities that connect multiple sites to provider hub devices through overlay tunnels in an SD-WAN deployment. To create a provider hub site, you need to select a Point of Presence (POP) and at least one provider hub device associated with the POP. This makes it possible to add provider hubs when you create spoke and enterprise sites so that, the sites can backhaul traffic to the provider hub devices and to the internet. The Tenant Administrator must add provider hub sites to connect a cloud branch site with provider hub devices.

NOTE: The OpCo or Service Provider Administrator must provision provider hub devices with DATA_ONLY or OAM_AND_DATA capabilities before tenants can add provider hub sites. The Tenant Administrator cannot provision provider hub devices.

To add a provider hub site:

1. Select **Resources > Site Management**.

The Sites page appears.

2. Click **Add** and select **Add Provider Hub**.

The **Add Provider Hub for *Tenant-Name*** page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 23 on page 104](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the **Sites** page where the newly added provider hub site is listed, with the Site Name displaying the provider hub device's name and Site Status displaying **Provisioned**.

Table 23: Fields on the Provider Hub for Tenant-Name Page

Field	Description
Configuration	
Service POP	Select a POP for the site. A service POP is a location at which a service provider instantiates a network function, such as a virtualized network function (VNF).
Hub Device Name	Select either a single provider hub device or multiple provider hub devices from the dropdown menu. If you select multiple provider hubs, the CSO provisions the provider hub sites in the order in which you selected provider hub devices. Provider hub devices with DATA_ONLY and OAM_AND_DATA capabilities are listed.

RELATED DOCUMENTATION

About the Site Management Page 68
About the Site Groups Page 216

Adding Cloud Spoke Sites for SD-WAN Deployment

A cloud spoke represents an automation endpoint (virtual machine (VM) or an EC2 Instance) running a Juniper Networks vSRX image in the Amazon Web Services(AWS) virtual private cloud (VPC). The cloud spoke sites are connected to the hub sites using the overlay connections. You create a cloud spoke site from the **Sites** page. This topic describes how to add a cloud spoke site for a tenant.

NOTE:

- You can add a cloud spoke site only in hub-and-spoke topology.
- To ensure that only hub-and-spoke topology is created, we recommend you to disable the DVPN configuration while adding the tenant.
- You cannot add a cloud spoke site in full mesh topology.
- Only the tenants with SD-WAN Advanced service level can create a cloud spoke site.

To add a cloud spoke site:

1. Select **Resources > Site Management**.

The Sites page appears.

2. Click **Add** and select **Cloud Spoke**.

The **Add Cloud Spoke Site** page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 24 on page 105](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Review the configuration and modify the settings, if needed, from the **Summary** tab.

5. Click **OK**.

The newly added cloud spoke site is displayed on the **Sites** page.

Table 24: Fields on the Add Cloud Spoke Site Page

Field	Description
General	

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Site Information	
Site Name	<p>Enter a unique name for the site. Enter a unique string of alphanumeric characters and special character (-). The maximum length is 32 characters.</p> <p>Example: aws-cloud-spoke</p>
Device Host Name	<p>The device host name is auto-generated and uses the format <i>tenant-name.host-name</i>. You cannot change the <i>tenant-name</i> part in the device host name. Use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.</p>
Site Group	<p>(Optional) Select a site group to which you want to assign the site.</p> <p>Example: cloud-spoke</p>
Site Capabilities	<p>NOTE: Only the tenants with SD-WAN Advanced service level can create a cloud spoke site.</p> <p>The Secure SD-WAN Advanced option is selected automatically.</p>
Address and Contact Information	
Street Address	Enter the street address of the site.
City	Enter the name of the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	<p>Select the country where the site is located.</p> <p>You can click the Validate button to verify the address that you specified:</p> <ul style="list-style-type: none"> • The Site address verification successful message is displayed if the address can be verified. You can click the View location on a map link to see the address location. • If the address cannot be verified, the Site address could not be validated message is displayed .
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Phone	Enter the phone number of the contact person for the site.
Advanced Configuration	
Domain Name Server (DNS)	Enter one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Enter the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers. Example: ntp.example.net The site must have DNS reachability to resolve the FQDN during site configuration.
Select Timezone	Select the time zone for the site. Click Next to continue.
Device	
Activation Code	If the automatic activation of the device is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.
Device Root Password	The default root password is fetched from the ENC_ROOT_PASSWORD field in the device template. You can retain the password or change it by entering a password in plain-text format. The password is encrypted and stored on the device.
Management Interface Family	Select IPv4 or IPv6.
Device Template	Click a device template to select the plan for WAN connectivity. A device template contains information such as device family, a list of SD-WAN features supported, and the number of links supported. NOTE: vSRX as SD-WAN spoke in AWS template supports cloud spoke site for AWS VPC.
Hub Configuration	
Primary Provider Hub	Select the hub site to which the spoke site must connect.
Secondary Provider Hub	Select a secondary hub site.
Cloud Information	

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Region	<p>Select the region to which the site belongs. The regions in CSO are mapped to the regions in the AWS account.</p> <p>Example: Ohio</p>
VPC ID	<p>Enter the VPC ID from the AWS account.</p> <p>To obtain VPC ID:</p> <ol style="list-style-type: none"> 1. Log in to your AWS account. 2. Search for the VPC service. 3. Click the VPC dashboard. 4. Select a VPC ID. <p>Ensure that the VPC is connected to an Internet gateway.</p> <p>To check whether VPC is attached:</p> <ol style="list-style-type: none"> 1. Log in to your AWS account. 2. Search for the VPC service. 3. Click the Internet Gateway dashboard. 4. Check whether the VPC state is attached. <p>Example: vpc-6d810314</p>
Management Subnet	<p>Specify whether CSO must create a new subnet or use an existing subnet from the AWS account. The management subnet of vSRX is used to push the initial stage-1 configuration. The following options are available:</p> <ul style="list-style-type: none"> • Use an existing subnet in AWS account • Create new
IP Prefix	<p>Enter the management IP prefix. The first four IP addresses in the subnet are reserved by AWS. For example, IP addresses x.x.x.0/x through x.x.x.3/x are always reserved by AWS. Hence, provide an IP address prefix other than the reserved IP address prefix.</p> <p>Example: 105.0.1.5/24</p>

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
WAN Links	
WAN_0 (ge-0/0/0) WAN_1 (ge-0/0/1)	Select the check boxes to configure the WAN links. You can configure up to two WAN links per site that support SD-WAN.
Link Type	Displays the connection type for WAN underlays. Only Internet link is supported.
Egress Bandwidth	Enter the maximum bandwidth (in Mbps) to be allowed for a specific WAN link.
Address Assignment Method	<p>Select the method of assigning an IP address to the WAN link—DHCP or STATIC.</p> <ul style="list-style-type: none"> • If you select DHCP, the IP address is provided by using the DHCP server of the service provider of the WAN link. • If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.
Static IP Prefix	<p>If you configure the address assignment method as STATIC, enter the private IPv4 address of the WAN link from the subnet. For example, if the IPv4 CIDR address is 105.0.2.0/24 for a WAN interface in the AWS account, then enter any IP address within the subnet. The first four IP addresses in the subnet are reserved by AWS. Hence, provide an IP prefix other than the reserved IP prefix.</p> <p>Example: 105.0.2.12/24</p>
Gateway IP Address	<p>If you configured the address assignment method as STATIC, enter the IPv4 address for the gateway of the WAN service provider. Typically, the first IP address in the subnet is selected for gateway IP address.</p> <p>Example: 105.0.2.1</p>
Elastic IP	<p>Elastic IP address is a public, static IPv4 address designed for dynamic cloud computing. The public IP address is mapped to the private subnet IP using one-to-one NAT. You must allocate the IP addresses based on the number of WAN links that are enabled. For example, If two WAN links are enabled, then you must allocate two elastic IP addresses.</p> <p>Example: 34.213.255.184</p>
Advanced Settings	Based on the connectivity requirement, the following fields are populated:
Provider	Enter the name of the service provider (SP).

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Cost/Month	Enter the cost per month of the subscribed bandwidth in the specified currency. In bandwidth-optimized SD-WAN, this information is used to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.
Link Priority	Enter a value in the range 1-255. A lower value indicates a more preferred link. A value of 1 indicates highest priority and a value of 255 indicates lowest priority. If you do not enter a value, the link priority is considered as 255.
Enable Local Breakout	<p>Click the toggle button to enable or disable (default) local breakout on the WAN link.</p> <ul style="list-style-type: none"> • If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent. • If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.
Breakout Options	Select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Autocreate Source NAT Rule	<p>If the WAN link is enabled for local breakout, you can click the toggle button to automatically create an interface-based source NAT rule on the WAN link. The automatically-created source NAT rule is implicitly defined and applied to the site and is not visible on the NAT Policies page.</p> <p>By default, this field is disabled.</p> <p>NOTE: If this option is enabled for a WAN interface W1 during the site addition workflow, a series of NAT source rules are automatically created. Each automatically created NAT rule is from a zone to the WAN interface, with a translation of type interface. Each pair of [zone - interface] represents a rule-set.</p> <p>For example, the following zone to W1 interface rule-set might be created:</p> <pre>Zone1 --> W1: Translation=Interface Zone2 --> W1: Translation=Interface Zone3 --> W1: Translation=Interface</pre> <p>To manually override any of these rules, you can create a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant zone and WAN interface as the source and destination. For example:</p> <pre>Zone1 --> W1 : Translation=Pool-2</pre> <p>The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.</p> <p>You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:</p> <pre>Zone1, Port 56578 --> W1: Translation=Pool-2</pre>
Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
BGP Underlay Options	<p>NOTE: This setting can be configured only if IPv4 address assignment (with STATIC as the address assignment method) and local breakout are enabled for the WAN link.</p> <p>Click the toggle button to enable BGP underlay routing.</p> <p>When you enable BGP underlay routing, route advertisements to the primary PE node and, if configured, the secondary PE node occur as follows:</p> <ul style="list-style-type: none"> • CSO advertises the WAN interface subnet. • If you configured pool-based translation, CSO advertises the NAT address pool. <p>NOTE: If underlay BGP is enabled for a WAN link, then the routes learnt from BGP are installed for local breakout; CSO does not generate the static default route.</p>
Primary Neighbor	Displays the IP address that you entered for the gateway for the WAN link.
Secondary Neighbor	<p>If you want to provide PE resiliency, you can configure a secondary PE node.</p> <p>Enter the IP address of the secondary PE node.</p> <p>NOTE: If the primary PE node goes down, then the secondary PE is used as the next hop. When the primary PE comes back up, the route next hops are changed to the primary PE.</p>
eBGP Peer-AS-Number	<p>Enter the autonomous system (AS) number for the external (EBGP) peer.</p> <p>NOTE: If the peer AS number is not configured or the peer AS number that is configured is the same as that of the CPE site, then the BGP type is assumed to be internal BGP (IBGP).</p>
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> • None—Indicates that no authentication should be used. This is the default. • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Advertise Public LAN Prefixes	<p>Click the toggle button to enable the advertisement of public LAN prefixes. This field is disabled by default.</p> <p>If the tenant has a public IP address pool configured and you enable the advertisement of public LAN prefixes, then for LAN segments that are created with a subnet that falls under the tenant public IP address pool, CSO advertises the LAN subnet to the BGP underlay.</p> <p>NOTE: When public LAN advertisement is enabled for the WAN link, public LAN prefixes are advertised through the BGP underlay towards MPLS or the Internet. If a site has two versions of the route installed for the same LAN prefix in the overlay and underlay, the overlay routes are always preferred over underlay.</p>
Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Overlay Tunnel Type	<p>Select the mesh overlay tunnel type—GRE and GRE_IPSEC.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device	Displays the peer hub device to which the site is connected.
Overlay Peer Interface	Select the interface name of the hub device to which the WAN link of the site is connected.
Backup Link	<p>Select a backup link through which traffic can be routed when the primary links are unavailable. You cannot select the default link as the backup link. Note that you cannot assign the backup link for exclusive breakout traffic (the Use only for breakout traffic option). If local breakout is enabled for the site, the breakout traffic is also routed through the backup link when the breakout link is not available.</p> <p>When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. However, note that the SLA data is not monitored for the backup link.</p>
Default Links	<p>Select the default links that must be used for routing traffic. The site can have multiple default links to the hub site as well as to the Internet.</p> <p>Default links are used primarily for overlay traffic but can be used for local breakout traffic as well. A default link cannot be used exclusively for local breakout traffic. The default link is optional and in case it is not chosen, all links are used through equal-cost multipath (ECMP).</p>

Table 24: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Management Connectivity	
OAM IP Prefix	<p>Enter an IPv4 address prefix (such as 10.100.100.11/32) for the loopback interface on the CPE device. The IP address prefix should be a /32 IP address prefix and must be unique across the entire management network.</p> <p>NOTE: We recommend that you do not configure this setting (leave the IP Prefix field blank) because management connectivity is handled automatically by CSO.</p>
DVPN Threshold for Tunnel Creation	<p>Enter the maximum number of sessions closed between the connected sites in a duration of two minutes at which full mesh is created between the two sites.</p> <p>The default value is 5.</p> <p>For example, if you specify the number of sessions as 5, dynamic mesh tunnels are created if the number of sessions closed between two branch sites in 2 minutes exceeds 5.</p>
DVPN Threshold for Tunnel Deletion	<p>Enter the number of sessions closed between the connected sites in a duration of 15 minutes below which full mesh is deleted between the two sites.</p> <p>The default value is 8.</p> <p>For example, if you specify the number of sessions closed as 8, dynamic mesh tunnels are deleted if the number of sessions closed is lesser than or equal to 8.</p>
LAN	Add at least one LAN segment.
LAN Segment	<p>Displays the LAN segment that you configure on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. See Table 25 on page 114.</p>

Table 25: Fields on the Add LAN Segment Page

Field	Description
Add LAN Segment	
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters. No spaces are allowed and the maximum length is 15 characters.</p>

Table 25: Fields on the Add LAN Segment Page (*continued*)

Field	Description
Department	<p>Select a department to which the LAN segment is to be assigned.</p> <p>Alternatively, click the Create Department link to create a new department and assign the LAN segment to it. See “Add a Department” on page 783 for details.</p> <p>You group LAN segments as departments for ease of management and for applying policies at the department-level.</p>
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.
CPE Ports	<p>Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment:</p> <ul style="list-style-type: none"> • CPE ports that you can include in the LAN segment are listed. <p>Select the ports from the Available column and click the right-arrow to move the ports to the Selected column.</p> <p>NOTE: You can select only one port if the CPE is an SRX Series device.</p>

RELATED DOCUMENTATION

[Provisioning a Cloud Spoke Site in AWS VPC | 115](#)
[About the Site Management Page | 68](#)
[About the Site Groups Page | 216](#)

Provisioning a Cloud Spoke Site in AWS VPC

IN THIS SECTION

- [Add a Cloud Spoke Site | 116](#)
- [Download the Cloud Formation Template | 117](#)
- [Provision the Device on AWS Server | 117](#)
- [Activate the Device | 118](#)

Use the following high-level steps to provision a vSRX cloud spoke site in Amazon Web Services (AWS) virtual private cloud (VPC).

Before you begin:

- Set up your Amazon Web Services (AWS) account.
- Identify the virtual private cloud (VPC) in which the AWS spoke site must be provisioned.
- Install licenses to use vSRX features. Choose any of the following AWS vSRX Image Licenses.
 - Bring Your Own License (BYOL)— If you plan to use a BYOL, then you must install the license on the device before deploying CSO SD-WAN functionality. See <https://aws.amazon.com/marketplace/pp/B01LYWCGDX>.
 - License included. See <https://aws.amazon.com/marketplace/pp/B01NAUWN0G>.
- Ensure that you have the supported software version for the AWS spoke.
- Reserve two elastic IP (public IP) addresses on AWS.

To set up and monitor your network:

Add a Cloud Spoke Site

To add a cloud spoke site:

1. Select **Resources > Site Management**.

The Sites page appears.

2. Click **Add > Add Cloud Spoke**.

The **Add Cloud Spoke Site** page appears.

3. Specify the site information such as, site name, AWS region, VPC ID, management subnet, IP prefix and click **Next**.
4. Specify vSRX as SD-WAN spoke in AWS as the device template.

NOTE:

- Only hub-and-spoke topology is supported for AWS cloud spoke site.
- Only Internet link is supported for WAN underlay connections.

5. Provide the WAN details and click **Next**.

The WAN traffic page appears, displaying a set of values for the WAN link configuration.

6. Specify additional requirements and click **Next**.
7. Specify LAN segment information and click **Next**.
8. In the **Summary** tab, check the configuration and click **Edit** to modify the settings.
9. Click **OK** to save the changes.

The new cloud spoke site that you created appears in the Sites page.

Download the Cloud Formation Template

To download the cloud formation template:

1. Click **Resources > Devices**.

The Devices List page appears.

2. Select the device and click **Cloud Info Template**.

The Cloud Info Template page appears.

3. Click **Download** to download the cloud formation template.

The template is downloaded to your local computer in JSON format.

Provision the Device on AWS Server

CSO creates cloud formation template with stage-1 configuration bundled in JSON format. You must download this template and then upload to AWS to provision the vSRX. The cloud formation template creates the required resources such as subnet, interface, vSRX and so on and applies the stage-1 configuration.

To provision the device on AWS server:

1. Log in to your AWS account.
 - If you have already logged in to your AWS account, the Create Stack page appears.
 - If you are not logged into your AWS account, a new Web page opens in your browser, displaying the AWS login information. Log in to your AWS account.

TIP: If you do not see the Create Stack page when you log in to or access your AWS account, then search for CloudFormation service.

The Create Stack page appears.

2. Select **CloudFormation** > **Stacks** > **Create Stack** > **Upload a template to Amazon S3**.
3. Click **Choose File** and select the cloud formation template that you downloaded in JSON format .
4. Click **Next**.
5. Specify the Stack name. For example, Oregonstack.
6. In the Parameters section, specify the KeyName for your EC2 instance.
7. Click **Next**.
8. Select **I acknowledge that AWS CloudFormation might create IAM Resources**.
9. Click **Create**.

The Create Stack pages displays a list of existing stacks and indicates that it is creating the stack that you requested. The create stack process takes up to 30 minutes. if the process does not complete in 30 minutes, a timeout occurs and you need to retry the process.

Activate the Device

To activate the device:

1. After the create stack process is complete, return to the Customer Portal and click **Next**.

The Activate Device page displays a status indicating that CSO is detecting the provisioning agent. This process takes up to 30 minutes. if the process does not complete in 30 minutes, a timeout occurs and you need to retry the process.

NOTE: You need not download the cloud formation template again. You can log in to the Customer Portal, access the Activate Device page, enter the activation code and click **Next**. After the CREATE_COMPLETE message is displayed on the AWS server, click Next on the Activate Device page to proceed with device activation.

If the spoke on AWS has been spawned successfully on AWS, it will contact CSO through outbound SSH connection. The device is detected and normal ZTP, process is triggered. The rest of the workflow is consistent with the normal on-premise workflow.

On Device Activation page, the device is activated through the following steps:

- Detecting the device
- Applying stage-one configuration to the device
- Bootstrapping of device
- Activating the device

After each successful step, you can see a green check mark. If any of these steps fails, a red exclamation mark appears.

2. After the activation process is complete, click **OK**.

The Sites page appears. To see the device activation status, hover over the device icon on the Sites page.

RELATED DOCUMENTATION

[Adding Cloud Spoke Sites for SD-WAN Deployment | 105](#)
[vSRX Deployment Guide for AWS](#)

Manually Adding Branch Sites

Starting from CSO Release 6.0.0, the branch site creation workflow is simplified by making the provisioning of services optional during the onboarding process. You can configure the services during the site creation or add the services later.

A branch site can be added with either SD-WAN or security services. For more information about adding a branch site with the following capabilities:

- SD-WAN, see [“Add a Branch Site with SD-WAN Capability” on page 120](#).

- Next-Generation Firewall, see [“Add a Standalone Next-Generation Firewall Site” on page 153](#).

To add a branch site without a service, see *Add Branch or Enterprise Hub Sites Without Provisioning a Service*.

Prerequisites to add a branch site are as follows:

- Ensure that the following ports are open in the network:
 - DNS Port 53
 - IPSEC-AH (IP Protocol 51)
 - IPSEC-ESP (IP Protocol 50)
 - NTP Port 123
 - UDP Ports 500 and 4500
- For an SRX cluster, ensure that the cluster is configured (physical cabling and cluster configuration) before onboarding the devices.
- For Zero Touch Provisioning (ZTP), ensure that the device can connect to the redirect server (redirect.juniper.net) by using the **ping** command.

Add a Branch Site with SD-WAN Capability

An on-premises spoke (branch) represents an endpoint that is part of customer premises equipment (CPE) at any physical location such as branch office or point of sale location. Typically, these points are connected using overlay connections to hub sites. You can add a branch site from the **Site Management** page.

The following device templates are supported for branch sites:

- NFX150 as SD-WAN CPE
- NFX250 as SD-WAN CPE
- Dual NFX250 as SD-WAN CPEs
- SRX as SD-WAN CPE
- Dual SRX as SD-WAN CPEs
- SRX4x00 as SD-WAN CPE
- Dual SRX4x00 as SD-WAN CPEs

From CSO release 5.4.0 onward, the branch site creation and site activation workflows can be optionally separated, giving more flexibility for on-site installation of customer premises equipment (CPE).

In SD-WAN deployments comprising single or dual customer premises equipment (CPE), tenant administrators have an option to enter the serial number of the CPE device(s) after adding the branch sites.

The branch site can be added by a tenant administrator and the CPE device associated with the site can be activated manually by another authorized user. The authorized user must enter either the serial number and the activation code, or only the serial number when manually activating the CPE device later. The option to add branch sites without serial number of a CPE device is applicable to both SRX and NFX (NFX150 and NFX250) device templates.

NOTE: In Dual CPE device templates, you cannot add serial number of one CPE and avoid entering serial number of the other CPE device. You can either enter serial numbers for both primary and secondary devices while creating the site or enter both serial numbers while activating the site.

Starting in Release 6.0.0, CSO supports the following SD-WAN services for a site:

- *Secure SD-WAN Essentials*—Provides the basic SD-WAN services. This service is ideal for small enterprises looking for managing simple WAN connectivity with comprehensive NGFW security services at the branch sites, using link-based application steering. The SD-WAN Essentials service allows Internet traffic to breakout locally, and thus avoids the need to backhaul web traffic over costly VPN or MPLS links. The sites support features such as intent-based firewall policies, WAN link management and control, CSO-controlled routing between sites connected through the static VPN, and site to site communication through MPLS or internet links behind NAT. A tenant with the SD-WAN Essentials service level can create only SD-WAN Essentials sites.

NOTE: You can upgrade a Secure SD-WAN Essentials site to a Secure SD-WAN Advanced site by editing the site information (allowed if the SD-WAN service level of the tenant is upgraded to Advanced).

- *Secure SD-WAN Advanced*—Provides the complete SD-WAN service. This service is ideal for enterprises with one or more data centers, requiring flexible topologies and dynamic application steering. Site-to-Site connectivity can be established by using a hub in a hub-and-spoke topology or through static or dynamic full mesh VPN tunnels. Enterprise wide intent based SD-WAN policies and service-level agreement (SLA) measurements allow CSO to differentiate and dynamically route traffic for different applications.
- SD-WAN sites on CSO Release 5.4.0 or earlier versions are treated as SD-WAN Advanced sites. You cannot downgrade the SD-WAN service level of a tenant from SD-WAN Advanced to SD-WAN Essentials.

Starting from CSO Release 6.0.0, the branch site creation workflow is simplified by making the provisioning of services optional during the onboarding process. You can configure the service during the site creation or add the service later. To add a branch site without the SD-WAN service, see *Add Branch or Enterprise Hub Sites Without Provisioning a Service*

To add a branch site with only SD-WAN capability:

1. Select **Resources > Site Management**.

The Sites page appears.

2. Click **Add** and select **Branch Site (Manual)**.

The **Add Branch Site** page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 26 on page 124](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. (Optional) You can review the configuration in the **Summary** tab and modify the settings, if required.

5. Click **OK**.

- If you entered a serial number during activation and automatic activation is enabled, the Site Activation Progress page appears. The site activation process proceeds through the tasks explained in *Troubleshooting Site Activation Issues*.

Click **OK** to close the Site Activation Progress page.

- If you did not enter a serial number and the automatic activation is disabled, you are returned to the Site Management page. CSO triggers a job and displays a confirmation message with a job link. Click the link to view the status of the job. After the job is finished, CSO displays a confirmation message with a job link. The status of the site changes to **CREATED**.

You must manually activate the device to finish the activation process.

NOTE: The following procedure is applicable if zero touch provisioning (ZTP) is set true in the device template. If ZTP is disabled in the device template, you must copy the stage-1 configuration and commit it on the device for CSO to proceed with the activation.

To manually activate the CPE (branch site) device:

- a. Select the branch site CPE that has to be activated.
- b. Click **Activate Site** link in the Site Management page.

The **Activate Site** page appears.

- c. Enter the serial number(s) of the device and the activation code. Click **OK**.

The **Site Activation Progress** page appears displaying the progress of steps executed for activating the CPE device. On successful activation of the device, the Site Status changes from **Created** to **Provisioned**.

- 6. If you have enabled the Zero Touch Provisioning field, CSO applies the stage-1 configuration automatically.

NOTE: The device is activated automatically, if you have already provided the activation code and device serial number while creating the firewall site.

If you have disabled the Zero Touch Provisioning field for the device, you must manually configure the stage-1 configuration on the device.

- a. Click the **Click to copy stage-1 config** link next to the Prestage Device task on the Site Activation Progress page. If you close the Site Activation Progress page inadvertently, you can access the page from the Site Management page. Click the **View** link next to the status of the site, under the Site Status column.

NOTE: You can also copy the configuration from the Devices page (Resources > Devices). Select the device and click **Stage1 Config**.

The Stage-1 Configuration page appears displaying the stage-1 configuration.

- b. Copy the stage-1 configuration.
- c. Log in to the device and enter Junos OS configuration mode.
- d. Paste the configuration that you copied and commit the configuration.

CSO applies the pre-script and stage-1 configuration (includes the device configuration). The status of the site changes to **MANAGED** on the Sites page.

If you selected SD-WAN Services while adding the device, then CSO generates the service provisioning configuration and applies it on the device. The site status changes to **PROVISIONED** in the Site Management page.

If you did not select SD-WAN Services while adding the device, then the device remains in the **MANAGED** state until you apply the service. You can edit the site and add the service. After you add the service, CSO applies the service provisioning configuration and the device is provisioned.

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability

Field	Description
General	
Site Information	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters.
Device Host Name	The device host name is auto-generated and uses the format <i>tenant-name.host-name</i> . You cannot change the <i>tenant-name</i> part in the device host name. Use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.
Site Group	Select a site group to which you want to assign the site.
Site Capabilities	<p>NOTE: Device Management, enabled by default, allows you to create a site with only device management capability (without any services) and add services later.</p> <p>To add an SD-WAN capability for this site, choose one of the following SD-WAN service types:</p> <ul style="list-style-type: none"> Secure SD-WAN Essentials—(Available for tenants with SD-WAN Essentials or Advanced service level) Provides basic SD-WAN services. The sites support features such as intent-based firewall policies, WAN link management and control, CSO-controlled routing between sites connected through the static VPN, and site to site communication through MPLS-based or internet-based links. The SD-WAN Essentials service does not support multihoming, dynamic mesh tunnels, cloud breakout profiles, SLA-based steering profiles, pool based source NAT rules, IPv6, MAP-E, or underlay BGP. Secure SD-WAN Advanced—(Available for tenants with SD-WAN Advanced service level) Provides complete SD-WAN services. This service level is ideal for enterprises with one or more data centers, requiring flexible topologies and dynamic application steering. Site-to-Site connectivity can be established by using a hub in a hub-and-spoke topology or through static or dynamic full mesh VPN tunnels. Enterprise wide intent based SD-WAN policies and service-level agreement (SLA) measurements allow to differentiate and dynamically route traffic for different applications.
Address and Contact Information	
Street Address	Enter the street address of the site.
City	Enter the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Country	<p>Select the country where the site is located.</p> <p>Click the Validate button to verify the address.</p> <ul style="list-style-type: none"> • The site address verification successful message is displayed if the address is verified. You can click the View location on a map link to see the address location. • If the address cannot be verified, the Site address could not be validated message is displayed .
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
Advanced Configuration	
Domain Name Server	<p>Specify one or more IPv4 or IPv6, or both IPv4 and IPv6 addresses of the DNS server. To specify more than one DNS server address, type the address, press Enter, and then type the next address, and so on.</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
Device	
<p>NOTE: Some fields in this section are displayed only if you enable the Device Redundancy option.</p>	

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Device Redundancy	<p>Disabled by default. Enable this option for dual CPEs.</p> <p>The following prerequisites are necessary for enabling device redundancy:</p> <ul style="list-style-type: none"> • Ensure that the control and fabric ports between both the nodes are connected. • Ensure that the device is preconfigured for management connectivity (factory-default or prestaged). Do not configure the control, fabric, and data (reth) ports as these ports will be reconfigured. <p>To identify the control, fabric, management, and data ports for each SRX model, refer to the SRX High Availability Configurator tool.</p> <p>NOTE: Do not generate the configuration in the tool as CSO generates and applies the cluster configuration automatically.</p> <ul style="list-style-type: none"> • If you are using ZTP on SRX300 and SRX320 devices, use ge-0/0/7 as the predefined DHCP port instead of ge-0/0/0. • Provide the fabric and data (reth) port information in the device template. The control and fxp0 ports are predefined. To change the control port, change it in the platform device template. To change the data (reth) port, change it in the SDWAN device template.
Device Series	<p>Select the device series to which the CPE belongs—SRX, NFX150, or NFX250.</p> <p>Based on the device series that you select, the supported device templates (containing information for configuring devices) are listed.</p> <p>Select a device template for the selected device series.</p>
Device Model	Select the device model number.
Device Root Password	The default root password is fetched from the ENC_ROOT_PASSWORD field in the device template. You can retain the password or change it by entering a password in plain-text format. The password is encrypted and stored on the device.

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Zero Touch Provisioning	<p>Click the toggle button to enable or disable Zero Touch Provisioning (ZTP). This option is enabled by default.</p> <p>To use ZTP, ensure the following:</p> <ul style="list-style-type: none"> Device must have connectivity to CSO and Juniper phone-home server (https://redirect.juniper.net) <p>Use telnet to verify connectivity:</p> <pre>telnet redirect.juniper.net:443 telnet CSO Hostname/IP:443</pre> <p>If the connection is established, the device has connectivity to the phone-home server and CSO.</p> <ul style="list-style-type: none"> Required certificates for phone-home server and CSO must be present on the device. <p>If ZTP is enabled, the Boot Image field is displayed and you must select an image that supports the Phone-Home client. During ZTP, the image on the firewall device is upgraded to the image that you select for the Boot Image.</p> <p>If you disable ZTP, ensure that the device has connectivity to CSO. If the device is not prestaged/preconfigured, then you must provide the details under the Management Connectivity section so that CSO can generate the configuration as part of the stage-1 configuration. You can skip the Management Connectivity section if the device has connectivity to CSO.</p> <p>If you disable ZTP, you must copy the stage-1 configuration from CSO and commit it on the device to start the onboarding process. Use any of the following options to copy the stage-1 configuration:</p> <ul style="list-style-type: none"> Click the Click to copy stage-1 config link next to Prestage Device task on the Site Activation Progress page. <p>If you close the Site Activation Progress page inadvertently, you can access the page from the Site Management page. Click the View link next to the status of the site under the Site Status column.</p> <ul style="list-style-type: none"> On the Devices page (Resources > Devices), select the device and click Stage1 Config.
Serial Number	<p>For a single CPE device, enter the serial number of the CPE device. Serial numbers are case-sensitive.</p> <p>If you do not enter serial number, the branch site is created but the CPE device associated with the site is not activated. See “Step-by-Step Procedure” on page 78 for more information.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Node 0 Serial Number	<p>For a dual CPE device, enter the serial number of the primary CPE device. The serial number is case sensitive.</p> <p>If you do not enter serial number, the branch site is created but the CPE device is not activated. See “Step-by-Step Procedure” on page 78 for more information.</p>
Node 1 Serial Number	<p>For a dual CPE device, enter the serial number of the secondary CPE device. The serial number is case sensitive.</p> <p>If you do not enter serial number, the branch site is created but the CPE device is not activated. See “Step-by-Step Procedure” on page 78 for more information.</p>
Is Cluster Already Formed?	<p>NOTE: This field is available only for SRX dual CPE devices.</p> <p>Click the toggle button to specify whether the SRX cluster has been manually formed (Yes) or not (No).</p>
Cluster ID	<p>NOTE: This field is available only for SRX dual CPE devices.</p> <p>If the SRX cluster hasn't been formed manually, specify a unique ID for the cluster.</p> <p>Range: 1 through 15</p> <p>If you've enabled ZTP for the site, the cluster is automatically formed when the site is activated. If you've disabled ZTP, the following processes are displayed on the Site Activation Progress page (that appears after you've added the branch site):</p> <ol style="list-style-type: none"> 1. After CSO models the site (that is, after the Model Site process completes successfully), click the Click to copy pre script link, which appears next to the Pre Script process. 2. Execute the commands as directed. <p>After the Pre Script process completes successfully, the SRX cluster is formed and the recovery.conf file is saved on the cluster. In case you want to delete the site later, you'll need this file to remove the stage-1 configuration and other configurations pushed to the device by CSO.</p> <ol style="list-style-type: none"> 3. Manually configure the stage-1 configuration on the primary device in the cluster. See “Step-by-Step Procedure” on page 123. <p>After the cluster is detected, CSO executes the bootstrap and provisioning processes and completes provisioning the cluster.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Auto Activate	Click the toggle button to enable or disable automatic activation of the CPE device. If you disable automatic activation, refer "Activate a Device" on page 252 topic to manually activate the CPE.
Activation Code	If the automatic activation of the device is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.
Node 0 Activation Code	If the automatic activation of dual CPEs is disabled, enter the activation code to manually activate the primary CPE device.
Node 1 Activation Code	If the automatic activation of dual CPEs is disabled, enter the activation code to manually activate the secondary CPE device.
Boot Image	Select the boot image from the drop-down list if you want to upgrade the image for the CPE device. The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process. If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image (NFX or SRX) is populated based on the device template that you have selected while creating a site. See <i>Uploading a Device Image</i> .
(Device Template)	Select a device template, which contains information for configuring a device.

Management Connectivity

NOTE: This section is displayed only when Zero Touch Provisioning is disabled. If you are adding a chassis cluster, then you must provide the interface details for both the nodes.

Address Family	Select IPv4 or IPv6.
Interface Name	This is the WAN interface that the device uses to connect to CSO.
Address assignment	DHCP is selected by default. If you want to provide a static IP address, select STATIC.
Management VLAN ID	Enter a VLAN ID for the WAN link. Range: 0 through 4094
PPPoE	Click the toggle button to enable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet).

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Hub Configuration	
<p>NOTE: Hub selection is optional for both SD-WAN Advanced and Essentials sites. SD-WAN Essentials sites do not support multihoming. However, you can edit an Essentials site (post activation) to upgrade it to an Advanced site and add a secondary hub later if required, provided that the tenant's service level is upgraded to Advanced.</p> <p>You can connect a Secure SD-WAN Advanced branch site only to Secure SD-WAN Advanced enterprise hubs.</p>	
Primary Provider Hub	Select the primary hub site to which this branch site must connect.
Secondary Provider Hub	<p>NOTE: Not applicable to sites with the Secure SD-WAN Essentials service.</p> <p>Select the secondary hub site to which this site must connect.</p> <p>This site connects to the secondary data hub site when the primary data hub is not reachable.</p>
Primary Enterprise Hub	Select the enterprise hub with which you want to connect the branch site. If you specify an enterprise hub, then the initial site-to-site traffic as well as the central breakout (backhaul) traffic (if applicable) is sent through the enterprise hub instead of the hub site.
Secondary Enterprise Hub	<p>NOTE: Not applicable to sites with the Secure SD-WAN Essentials service.</p> <p>Select the secondary enterprise hub for this branch site.</p> <p>The branch site connects with secondary enterprise hub when the primary enterprise hub is not reachable.</p>
Use Mesh Tags to connect EHub	<p>This toggle button is enabled by default. If this button is enabled, CSO uses mesh tags to automatically form the overlay tunnel between the site and the enterprise hubs.</p> <p>Disable this toggle button if you want to manually create static tunnel (per WAN link) between the branch site and the enterprise hubs. If you disable this option, you must manually enable at least one WAN link to connect to the enterprise hub by using the Connects to Enterprise Hubs toggle button in the Advanced Settings of the WAN link.</p>

WAN Links

NOTE: In Release 6.1.0, CSO moves a site to the PROVISIONED state when at least one of the WAN links obtains the IP address and is activated. You can activate the remaining DHCP WAN links later. If the provisioned site establishes Dynamic VPN (DVPN) tunnels to other sites before the DHCP WAN links are activated, then these DHCP WAN links participate in DVPN only when the tunnels are deleted and added back (that is, traffic between a pair of sites falls below the delete threshold, and then crosses the create threshold again).

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
WAN_0 <i>WAN-Interface-Name</i>	<p>This field is enabled by default.</p> <p>Enter parameters related to WAN_0. Fields marked with an asterisk (*) must be configured to proceed.</p>
Link Type	Select whether the link is an MPLS link or Internet link.
Access Type	<p>Select the access type for the underlay link.</p> <p>You can select the LTE, ADSL, or VDSL access type only for one WAN link.</p> <p>NOTE:</p> <ul style="list-style-type: none"> You cannot configure: <ul style="list-style-type: none"> LTE as the access type if you are using the dual SRX or dual NFX device templates. ADSL or VDSL as the access type if you are using the dual SRX, or the single or dual NFX device templates. <p>Ethernet is configured as the access type for the underlay link.</p> <ul style="list-style-type: none"> SRX300 does not support LTE and ADSL access types. On SRX300 line of Services Gateways (except SRX300 devices) and NFX150 devices, the LTE WAN link is supported through a SIM card that is inserted in the SIM slot of the Mini-Physical Interface Module (Mini-PIM). On NFX250 devices, the LTE WAN link is supported through a USB dongle (Vodafone K5160 dongle) that is plugged into the USB port of the CPE device. CSO supports the following combination of MPLS tunnels (with ADSL or VDSL access types) for a branch device: <ul style="list-style-type: none"> From the branch site (with an ADSL or VDSL access type) to an enterprise hub, provider hub, or a branch site (with Ethernet link). From the branch site (with an ADSL or VDSL access type) to another branch site (with an ADSL or VDSL link).

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
PPPoE/PPP	<p>Click the toggle button to enable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet) or PPP (Point-to-Point Protocol). By default, this toggle button is disabled.</p> <p>PPPoE works with Ethernet, ADSL, and VDSL access types while PPP works with the LTE access type.</p> <p>NOTE: This toggle button is not available for Internet links with LTE as the access type.</p> <p>You can enable PPPoE or PPP per WAN link. If you've enabled this toggle button, you must specify the PPPoE or PPP parameters (username, password, and authentication protocol) for the PPPoE or PPP server, respectively. The PPPoE or PPP server assigns an IP address to the WAN link after successful authentication. For more information, see the <i>PPPoE/PPP Settings</i> section in this table. You can enable PPPoE or PPP on MPLS-based or internet-based WAN links.</p> <p>If you've disabled this toggle button, select a method (DHCP or STATIC) to assign an IP address to the WAN link from the Address Assignment list.</p>
Access Point Name (APN)	<p>The access point name (APN) determines the Packet Data Network Gateway (P-GW) that the CPE device must use to connect to the Packet Data Network (PDN) such as Internet. All CPE devices are shipped with default APN settings. However, if you choose to use a private APN with the current LTE service provider or to use a different LTE service provider, enter the APN for the CPE device (as specified by the service provider) in this field.</p> <p>This field is displayed only if you have enabled PPPoE/PPP for MPLS links with LTE as the access type. If you have disabled PPPoE/PPP for these links, CSO uses the default APN settings.</p>
Egress Bandwidth	<p>Enter the maximum bandwidth, in Mbps, allowed on the WAN link.</p> <p>Range: 1 through 10,000.</p> <p>NOTE: This option is not available for Internet and MPLS links with LTE access type.</p>
<i>Underlay Address Families</i>	
IPv4	<p>Click the toggle button to enable or disable IPv4 address assignment for the WAN link. By default, IPv4 address assignment is enabled for the WAN link.</p> <p>The WAN link requires an IPv4 address to connect to an IPv4 network.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Address Assignment Method	<p>Select the method of assigning an IPv4 address to the WAN link—DHCP (Dynamic Host Configuration Protocol) or STATIC.</p> <p>This field is displayed only if you have disabled the PPPoE/PPP toggle button.</p> <p>If you select STATIC, you must provide the IPv4 address prefix and the gateway IPv4 address for the WAN link.</p> <p>NOTE: For Internet and MPLS links with LTE access type, you can select only DHCP for address assignment.</p>
Static IP Prefix	If you've configured the address assignment method as STATIC, enter the IPv4 address prefix of the WAN link.
Gateway IP Address	If you've configured the address assignment method as STATIC, enter the IPv4 address of the gateway of the WAN service provider.
IPv6	<p>Click the toggle button to enable or disable IPv6 address assignment for the WAN link. By default, IPv6 address assignment is disabled for the WAN link.</p> <p>The WAN link requires an IPv6 address to connect to an IPv6 network.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • IPv6 address assignment is supported only for sites with Secure SD-WAN Advanced service. • You cannot enable IPv6 address assignment for NFX250 devices.
Address Assignment Method	<p>Select the method of assigning an IPv6 address to the WAN link—DHCP (Dynamic Host Configuration Protocol - router advertisement only), STATIC, or SLAAC (Stateless Address Auto Configuration).</p> <p>This field is displayed only if you've disabled the PPPoE/PPP toggle button.</p> <p>If you select STATIC, you must provide the IPv6 address prefix and the gateway IPv6 address for the WAN link.</p> <p>NOTE: For Internet and MPLS links with LTE access type, you can select only DHCP for address assignment.</p>
Static IP Prefix	If you've configured the address assignment method as STATIC, enter the IPv6 address prefix of the WAN link.
Gateway IP Address	If you've configured the address assignment method as STATIC, enter the IPv6 address of the gateway of the WAN service provider.

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
WAN Link (Primary or Secondary)	For dual CPE device templates, displays whether the WAN link is a primary link or a secondary link. You cannot modify this field.
<i>Advanced Settings</i>	
Address Family (Tunnel Creation)	Select the underlay address family (IPv4 or IPv6) that is used to establish the overlay tunnel. The options on the list are populated based on the address family that you've configured for the underlay (either IPv4 or IPv6, or both).
Provider	<p>Enter the name of the service provider (SP) providing the WAN service.</p> <p>Only alphanumeric characters and '_', '@', '.', '/', '#', '&', '+', and '-' are allowed. The maximum number of characters allowed is 15.</p>
Cost/Month	<p>Enter the cost for using the WAN link per month and select the currency in which the cost is indicated from the adjacent drop-down list.</p> <p>Range: 1 through 10,000.</p> <p>In bandwidth-optimized SD-WAN, CSO uses this information to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.</p>
Link Priority	Enter a value in the range 1-255. A lower value indicates a more preferred link. A value of 1 indicates highest priority and a value of 255 indicates lowest priority. If you do not enter a value, the link priority is considered as 255.
Enable Local Breakout	<p>Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent. • If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.
Breakout Options	Select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
MAP-E	<p>Click the toggle button to enable or disable the Mapping of Address and Port with Encapsulation (MAP-E) functionality on the IPv6 WAN link. By default, MAP-E is disabled.</p> <p>MAP-E supports transporting IPv4 packets across an IPv6 network by using IPv4-in-IPv6 encapsulation.</p> <p>For more information on MAP-E, see Mapping of Address and Port with Encapsulation on NFX Series Devices.</p> <p>NOTE:</p> <ul style="list-style-type: none"> MAP-E is compliant only with the Japan Network Enabler (JPNE) standards. CSO supports MAP-E only on one WAN link of the branch site (Secure SD-WAN Advanced service only) with NFX150 as the CPE. IPV6 address assignment and local breakout must be enabled for the WAN link.
Autocreate Source NAT Rule	<p>NOTE: Sites with Secure SD-WAN Essentials service support interface-based source NAT rules only. If you enable this options for an SD-WAN Essentials site, interface-based source NAT rules are automatically applied. If you enable this options for an SD-WAN Advanced site, you must select a source NAT rule from the Translation field.</p> <p>Click the toggle button to enable or disable the automatic creation of source NAT rules. By default, this field is enabled when IPv4 address assignment and local breakout are enabled for the WAN link.</p> <p>Table 27 on page 144 explains how source NAT rules are automatically created on the WAN link. The automatically-created source NAT rules are implicitly defined and applied to the site and is not visible on the NAT Policies page.</p> <p>NOTE: You can manually override automatically created NAT rules, by creating a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant department zone and WAN interface as the source and destination. For example:</p> <pre>Dept-Zone1 --> W1 : Translation=Pool-2</pre> <p>The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.</p> <p>You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:</p> <pre>Dept-Zone1, Port 56578 --> W1: Translation=Pool-2</pre>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Translation	<p>NOTE: This field is displayed only if the automatic creation of source NAT rules is enabled for the WAN link, and the SD-WAN service used is Advanced. Sites with Secure SD-WAN Essentials service support interface-based source NAT rules only.</p> <p>Select the type of NAT to use for the traffic on the WAN link:</p> <ul style="list-style-type: none"> • Interface—Use interface-based NAT, which is the default. • Pool—Use pool-based NAT. If you select this option, you must specify the IP addresses that are to be used for the NAT pool. <p>NOTE: No NAT is performed for tenant-owned public IP addresses.</p>
IP Addresses	For pool-based NAT, enter one or more IP addresses, subnets, or an IP address range. Separate multiple IP addresses by using commas and use a hyphen to denote a range; for example, 192.0.2.1-192.0.2.50.
Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the most preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>
BGP Underlay Options	<p>NOTE: Not applicable to sites with SD-WAN Essentials service.</p> <p>NOTE: This setting can be configured only if IPv4 address assignment (with STATIC as the address assignment method) and local breakout are enabled for the WAN link.</p> <p>Click the toggle button to enable BGP underlay routing.</p> <p>When you enable BGP underlay routing, route advertisements to the primary PE node and, if configured, the secondary PE node occur as follows:</p> <ul style="list-style-type: none"> • CSO advertises the WAN interface subnet. • If you configured pool-based translation, CSO advertises the NAT address pool. <p>NOTE: If underlay BGP is enabled for a WAN link, then the routes learnt from BGP are installed for local breakout; CSO does not generate the static default route.</p>
Primary Neighbor	Displays the IP address that you entered for the gateway for the WAN link.
Secondary Neighbor	<p>If you want to provide PE resiliency, you can configure a secondary PE node.</p> <p>Enter the IP address of the secondary PE node.</p> <p>NOTE: If the primary PE node goes down, then the secondary PE is used as the next hop. When the primary PE comes back up, the route next hops are changed to the primary PE.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
eBGP Peer-AS-Number	<p>Enter the autonomous system (AS) number for the external (EBGP) peer.</p> <p>NOTE: If the peer AS number is not configured or the peer AS number that is configured is the same as that of the CPE site, then the BGP type is assumed to be internal BGP (IBGP).</p>
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> • None—Indicates that no authentication should be used. This is the default. • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.
Auth Key	<p>If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.</p>
Advertise Public LAN Prefixes	<p>Click the toggle button to enable the advertisement of public LAN prefixes. This field is disabled by default.</p> <p>If the tenant has a public IP address pool configured and you enable the advertisement of public LAN prefixes, then for LAN segments that are created with a subnet that falls under the tenant public IP address pool, CSO advertises the LAN subnet to the BGP underlay.</p> <p>NOTE: When public LAN advertisement is enabled for the WAN link, public LAN prefixes are advertised through the BGP underlay towards MPLS or the Internet. If a site has two versions of the route installed for the same LAN prefix in the overlay and underlay, the overlay routes are always preferred over underlay.</p>
Use For Fullmesh	<p>Click the toggle button to specify whether the WAN link can be a part of a fullmesh topology.</p> <p>A site with a single-CPE device can have a maximum of three WAN links enabled for meshing and a site with dual-CPE devices can have a maximum of four WAN links enabled for meshing.</p> <p>NOTE: Even if you enable this field, sites with SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or the Tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Mesh Overlay Link Type	<p>When Use for Fullmesh field is enabled, select the type of mesh overlay link—GRE and GRE_IPSEC.</p> <p>If the link type is Internet, by default, the value for mesh overlay link type is GRE_IPSEC.</p> <p>If the link type is MPLS, select one of the following options:</p> <ul style="list-style-type: none"> • GRE-IPSEC • GRE <p>NOTE: If you've enabled IPv6 address assignment for the WAN links, you can select only GRE-IPSEC as the type of mesh overlay link.</p>
Mesh Tag	<p>When the Use for Fullmesh field is enabled, enter the tag to be associated with the WAN link for creating tunnels. You can assign only one tag to the link.</p> <p>Matching mesh tags is one of the criteria used to form tunnels between sites that support meshing.</p> <ul style="list-style-type: none"> • For a branch site, you can select one mesh tag. • For an enterprise hub you can select one or more mesh tags. <p>For more information about mesh tags, see “Mesh Tags Overview” on page 240.</p>
Connects to Enterprise Hubs	<p>This field is displayed only if you have enabled the Use Mesh Tags to Connect EHub field in the Hub Configuration section.</p> <p>Enable this toggle button if you want to manually connect the site to an enterprise hub, without using mesh tags.</p>
Primary EHub Tunnel Type	<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the tunnel type to be used for the connection between the branch site and the primary enterprise hub.</p>
Primary EHub Peer Device	<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Displays the name of the primary enterprise hub you have selected.</p>
Primary Ehub Peer Interface	<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the primary enterprise hub WAN link that needs to be part of the tunnel. You can select multiple WAN links.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Secondary EHub Tunnel Type	<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the tunnel type to be used for the connection between the branch site and the secondary enterprise hub.</p>
Secondary EHub Peer Device	<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Displays the name of the secondary enterprise hub you have selected.</p>
Secondary Ehub Peer Interface	<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the secondary enterprise hub WAN link that needs to be part of the tunnel. You can select multiple WAN links.</p>
Connects to Provider Hubs	<p>NOTE: The Connects to Provider Hubs field is available only if you have selected a provider hub.</p> <p>Click the toggle button to specify that the WAN link of the site connects to a hub.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted. • For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.
Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Overlay Tunnel Type	<p>This field is displayed when the Connects to Provider Hubs field is enabled and only one provider hub (primary) is specified.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) of the tunnel to the hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device	<p>This field is displayed when the Connects to Provider Hubs field is enabled and only one provider hub (primary) is specified.</p> <p>Displays the peer hub device to which the site is connected.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Overlay Peer Interface	<p>This field is displayed when the Connects to Provider Hubs field is enabled and only one provider hub (primary) is specified.</p> <p>Select the interface name of the hub device to which the WAN link of the site is connected.</p>
Overlay Tunnel Type 1	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) for the tunnel to the primary hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device 1	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Displays the primary peer hub device to which the site is connected.</p>
Overlay Peer Interface 1	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the interface name of the primary hub device to which the WAN link of the site is connected.</p>
Overlay Tunnel Type 2	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) for the tunnel to the secondary hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device 2	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Displays the secondary peer hub device to which the site is connected.</p>
Overlay Peer Interface 2	<p>This field is displayed when the Connects to Provider Hubs field is enabled and both primary and secondary hubs are specified.</p> <p>Select the interface name of the secondary hub device to which the WAN link of the site is connected.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Backup Link	<p>Select a backup link through which traffic can be routed when the primary (other) links are unavailable. You can select any link other than the default links or links that are configured exclusively for local breakout traffic.</p> <p>When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. However, SLA data is not monitored for the backup link.</p>
Default Link	<p>Select one or more links that will be used for routing traffic in the absence of matching SD-WAN policy intents. A site can have multiple default links to the hub site.</p> <p>Default links are used primarily for overlay traffic but can also be used for local breakout traffic. However, a default link cannot be used exclusively for local breakout traffic. If you do not specify a default link, then equal-cost multipath (ECMP) is used to choose the link on which to route traffic.</p>
VLAN ID	<p>Enter a VLAN ID for the WAN link.</p> <p>Range: 0 through 4049 (4050 to 4094 is reserved by CSO).</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you are configuring more than one WAN link on the same physical interface, only one WAN link can be untagged; for the remaining WAN links, you must configure a VLAN ID. • A combination of tagged and untagged on the same physical interface is supported only for single CPE devices. • You cannot have a combination of tagged and untagged WAN links on the same et interface. If you are configuring multiple WAN links on the same et interface, then you must specify a VLAN ID for all the links.
WAN_1 <i>WAN-Interface-Name</i>	<p>Click the toggle button to enable or disable the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for <i>WAN_0 WAN-Interface-Name</i> for an explanation of the fields</p>
WAN_2 <i>WAN-Interface-Name</i>	<p>Click the toggle button to enable or disable the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for <i>WAN_0 WAN-Interface-Name</i> for an explanation of the fields</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
WAN_3 WAN-Interface-Name	Click the toggle button to enable or disable the WAN link. When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for WAN_0 WAN-Interface-Name for an explanation of the fields
PPPoE/PPP Settings	
Username	Enter the username, for the PPPoE server or PPP server, as specified by the service provider. For example, ISP-ANetwork.
Password	Enter the password for the PPPoE server or PPP server, as specified by the service provider.
Authentication Protocol	Select Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) for authentication, as specified by the service provider.
Advanced Configuration	
<p>NOTE: Sites with SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or a tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.</p>	
OAM IP Prefix	Enter an IPv4 address prefix (such as 10.100.100.11/32) for the loopback interface on the CPE device. The IP address prefix should be a /32 IP address prefix and must be unique across the entire management network. NOTE: We recommend that you do not configure this setting (leave the IP Prefix field blank) because management connectivity is handled automatically by CSO.
DVPN Threshold for Tunnel Creation	<p>NOTE: Not applicable to sites with SD-WAN Essentials service.</p> <p>Enter the maximum number of sessions closed between the connected sites in a duration of two minutes at which full mesh is created between the two sites.</p> <p>The default value is 5.</p> <p>For example, if you specify the number of sessions as 5, dynamic mesh tunnels are created if the number of sessions closed between two branch sites in 2 minutes exceeds 5.</p>

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
DVPN Threshold for Tunnel Deletion	<p>NOTE: Not applicable to sites with SD-WAN Essentials service.</p> <p>Enter the number of sessions closed between the connected sites in a duration of 15 minutes below which full mesh is deleted between the two sites.</p> <p>The default value is 8.</p> <p>For example, if you specify the number of sessions closed as 8, dynamic mesh tunnels are deleted if the number of sessions closed is lesser than or equal to 8.</p>

LAN Segment Configuration

Add LAN Segment	<p>You must add at least one LAN segment for a branch site. To add a LAN segment:</p> <ol style="list-style-type: none"> 1. Click the + icon. The Add LAN Segment page appears. 2. Complete the configuration settings according to the guidelines provided in Table 28 on page 146. 3. Click Save. The LAN segment is added and you are returned to the Add Site for <i>Tenant-Name</i> page.
-----------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Configuration Templates (Optional)

Table 26: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Configuration Templates List	<p>Select one or more configuration templates from the list. This list is filtered based on the device that you select.</p> <p>Configuration templates are stage-2 templates that are added by your OpCo administrators or SP administrators or Tenant administrators.</p> <p>NOTE: You must set the parameters of the configuration templates that you have selected before you move to the LAN section.</p> <p>To set the parameters for the selected configuration templates:</p> <ol style="list-style-type: none"> 1. After you select one or more configuration templates, click Set Parameters. The Device Configurations page appears. This page consists of two tabs—Configure and Summary 2. In the Configure tab fill in the attributes for each of the configuration templates. (Optional) View the CLI commands in the Summary tab. 3. Click Save. You have added and set the parameters for the configuration templates that are part of the site template that you are creating.

Table 27: Automatic Creation of Source NAT Rules

Autocreate Source NAT Rule	Translation	NAT Rules Creation
Disabled	Not applicable (No NAT)	None.

Table 27: Automatic Creation of Source NAT Rules (*continued*)

Autocreate Source NAT Rule	Translation	NAT Rules Creation
Enabled	Interface-Based (Default)—CSO creates interface-based NAT rules.	<p>Source NAT rules are automatically created, with each rule from a department zone to the WAN interface, with a translation of type interface. Each pair of [zone - interface] represents a rule-set.</p> <p>For example, the following department zone to (WAN link) W1 interface rule-set might be created:</p> <pre>Dept-Zone1 --> W1: Translation=Interface Dept-Zone2 --> W1: Translation=Interface Dept-Zone3 --> W1: Translation=Interface</pre> <p>When traffic from a branch site breaks out at an enterprise hub, a source NAT rule is automatically created at the enterprise hub from the department routing group (also referred to as VRF group) to the WAN interface.</p> <pre>Dept-vrf-group --> W1: Translation=Interface</pre>
Enabled	Pool-Based—CSO automatically creates pool-based NAT rules (Not applicable to sites with SD-WAN Essentials service).	<p>Source NAT rules are automatically created, with each rule from a department zone to the WAN NAT pool with a translation of type pool.</p> <p>For example, a source NAT rule from department zone to NAT pool might be created:</p> <pre>Dept-Zone1 --> W1 : Translation=Pool-1 Dept-Zone2 --> W1 : Translation=Pool-1</pre> <p>When traffic from a branch site breaks out at an enterprise hub, a source NAT rule is automatically created at the enterprise hub from the department routing group to the WAN pool.</p> <pre>Dept-vrf-group --> W1: Translation=Pool</pre>

Table 28: Fields on the Add LAN Segment page

Field	Description
Use for Overlay VPN	<p>Enable the Use for Overlay VPN field to associate the LAN segment with the selected department (VRF + ZONE) for overlay traffic to other sites.</p> <p>Disable the Use for Overlay VPN field to associate the LAN segment with a security zone for underlay breakout. You must define zone-based security policies.</p> <p>NOTE: When adding a new site, this field is enabled by default and cannot be modified. However, when you add a new LAN Segment to a provisioned site from the LAN tab of the Site-Name page, you can enable or disable this option.</p>
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length allowed is 15 characters.</p>
CPE Port	<p>NOTE: Applicable to SRX Series devices.</p> <p>Select the CPE port to be added in the LAN segment.</p> <p>When you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page, you can select (or create) a LAG interface or a redundant Ethernet (reth) interface (for dual CPE cluster) to connect the SRX Series CPE devices to an EX series switch.</p> <p>To use the et interface on SRX4600 devices, you must create a LAG interface and configure the et interface as a member of the LAG (aggregated Ethernet or ae) interface. See “Create LAG Interface” on page 312.</p> <p>For an SRX4600 dual CPE cluster, you can use the et interface if it is configured as a member of the redundant Ethernet (reth) interface.</p>
Add LAG Interface	<p>NOTE: This option is available when you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page.</p> <p>Click the link to create a LAG interface (ae interface) if you want to use it to connect the SRX Series CPE to the EX Series switch. See “Create LAG Interface” on page 312 for details.</p>
Create RETH Interface	<p>NOTE: This option is available when you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page.</p> <p>Click the link to create a reth interface for an SD-WAN site with a dual CPE cluster. See “Create a RETH Interface” on page 314 for details.</p>

Table 28: Fields on the Add LAN Segment page (*continued*)

Field	Description
Type NOTE: This field is displayed only for LAN segments associated with enterprise hub sites.	Select the type of LAN segment: <ul style="list-style-type: none"> • Directly Connected (default)—Indicates that the LAN segment is directly connected to the site. • Dynamic Routed—Indicates that the LAN segment is not directly connected to the site and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.
VLAN ID	Enter the VLAN ID for the LAN segment. By default, VLAN ID is set to 1 and native VLAN is enabled for untagged traffic. Range: 1 to 4049 .
Use for Native VLAN	Enable this option to use the VLAN ID specified above for untagged traffic. The CPE interface is configured with a native-vlan-id, which has the same value as the VLAN ID.
Department	NOTE: This field is available only if the Use for Overlay VPN field is enabled. Select a department to which the LAN segment is assigned. Alternatively, click the Create Department link to create a new department and assign the LAN segment to it. See “Add a Department” on page 783 for details. You can group LAN segments as departments for ease of management and for applying policies at the department-level. For LAN segments that are dynamically routed, you can assign only a data center department.
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment. This address will be the default gateway for endpoints in this LAN segment. For example: 192.0.2.8/24.
Zone	NOTE: This field is available only if the Use for Overlay VPN field is disabled. Select a security zone to be associated with this LAN segment. Alternatively click Create Zone to create a new security zone and assign that to this LAN segment. See “Adding a Security Zone” on page 318 for details.
DHCP	For directly connected LAN segments, click the toggle button to enable DHCP. You can enable DHCP if you want to assign IP addresses by using a DHCP server or disable DHCP if you want to assign a static IP address to the LAN segment. NOTE: If you enable DHCP, additional fields appear on the page.

Table 28: Fields on the Add LAN Segment page (*continued*)

Field	Description
Additional fields related to DHCP	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server. Default: 1440 Range: 0 through 4,294,967,295 seconds.
Name Server	Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address. NOTE: DNS servers are used to resolve hostnames into IP addresses.
CPE Ports	NOTE: Applicable to NFX150 and NFX250 devices. For sites with SD-WAN capability, the CPE Ports field is disabled and the CPE ports that you can include in the LAN segment are listed. Select the ports from the Available column and click the right-arrow to move the ports to the Selected column.
Static Routing	
Use this section to configure static routing on the LAN segment. Provide the IP addresses of all the LAN routers connected to the CPE device and the static subnets behind these routers.	
<i>Add LAN Router IP Prefix</i>	
LAN Router IP	Enter the IP address of the LAN router that is connected to the CPE device.
Prefix	Enter the subnets that are connected to the LAN router.
BFD	Enable Bidirectional Forwarding Detection (BFD) to detect any failures on the static route.

Table 28: Fields on the Add LAN Segment page (*continued*)

Field	Description
<i>Dynamic Routing</i>	
Routing Protocol	Enable this toggle button to configure dynamic routing using the BGP or OSPF protocol.
BFD	Enable Bidirectional Forwarding Detection (BFD) to detect any failures in the LAN segment.
Protocol	Select either BGP or OSPF.
<p>BGP Configuration</p> <p>NOTE: Starting in Release 6.1.0, CSO explicitly disables the long-lived graceful restart (LLGR) capability for BGP peering sessions with provider edge (PE) and data center or LAN routers. Disabling LLGR ensures that the CPE does not differentiate the route advertisements to the peering router irrespective of the peering router's LLGR capability.</p> <p>Prior to CSO Release 6.1.0, LLGR helper mode is enabled by default (implicit behavior of Junos OS) on the CPE for BGP peering towards PE router in IP VPN deployments, and data center or LAN routers in data center deployments.</p>	
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> • None—Indicates that no authentication should be used. This is the default. • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.
BGP Options	<p>You can select the following options based on your requirements:</p> <ul style="list-style-type: none"> • AS-OVERRIDE: Replaces all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer. • AS-PATH-PREPEND: Prepends one or more autonomous system (AS) numbers at the beginning of an AS path. Prepending an AS path makes a shorter AS path look longer and therefore it becomes less preferable to BGP. • AS-LOOP: Allows the local device's AS number to be added in the received AS paths. You can specify the number of times the detection of local AS is allowed in the AS path.
Loop Count	<p>This field is displayed only if you select AS-LOOP.</p> <p>Enter the maximum number of times the detection of local AS is allowed in the AS path.</p>

Table 28: Fields on the Add LAN Segment page (*continued*)

Field	Description
Peer IP Address	Enter the IP address of the LAN BGP peer.
Peer AS Number	Enter the autonomous system (AS) number of the LAN BGP peer. By default, CSO uses the AS number 64512. You can enter a different AS number.
Local AS Number	Enter the local AS number. When you configure this parameter, the local AS number is used for BGP peering instead of the global AS number configured for the CPE.
<i>OSPF Configuration</i>	
OSPF Area ID	Specify the OSPF area identifier to be used for the dynamic route.
Authentication	<p>Select the OSPF route authentication method to be used:</p> <ul style="list-style-type: none"> • Password—Indicates that password-based authentication should be used. If you choose this option, you must specify the password. (This is the default). • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key. • None—Indicates that no authentication should be used.
Password	Enter the password to be used to verify the authenticity of OSPF packets.
Confirm Password	Retype the password for confirmation purposes.
MD5 Auth Key ID	<p>If you specified that MD5 should be used for authentication, enter the OSPF MD5 authentication key ID.</p> <p>Range: 1 through 255.</p>
Auth Key	If you specified that MD5 should be used for authentication, enter an MD5 authentication key, which is used to verify the authenticity of OSPF packets.
<i>Route Advertisement Control</i>	
LAN Route(s) to Overlay	When this option is enabled, LAN routes are advertised to the remote CPEs. By default, this option is enabled.

Table 28: Fields on the Add LAN Segment page (*continued*)

Field	Description
Overlay Route(s) to LAN	<p>This option is displayed only if you enable the Routing Protocol toggle button. By default, this option is disabled.</p> <p>Enable this option to advertise the remote CPE routes received in a department to the LAN router.</p> <p>NOTE: In CSO Release 6.0.0 and earlier releases, this option is called Advertise LAN Prefix and is applicable only for data center departments.</p>
Static/Aggr Routes to Overlay	<p>Enable this option to allow advertisement of static or aggregate routes to the overlay network.</p> <ul style="list-style-type: none"> • If a large number of LAN routes are present, then you can disable the LAN Route(s) to Overlay option and use this option to advertise aggregate routes. • If you want to advertise additional routes, then you can enable the LAN Route(s) to Overlay option and use this option to advertise additional static routes.

RELATED DOCUMENTATION

[About the Site Management Page](#) | 68

Adding and Provisioning a Next Generation Firewall Overview

Overview

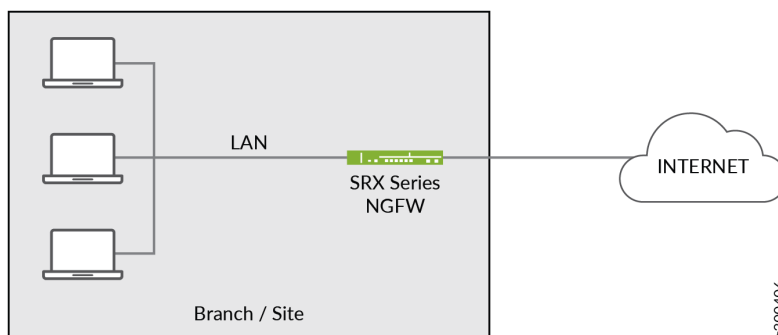
You can use Contrail Service Orchestration (CSO) to

- Add a firewall site for the next generation firewall device.
- Configure a CPE device (SRX Series services gateway) as a next generation firewall device.
- Add firewall policies for the standalone firewall site.
- Deploy the firewall policies for the standalone firewall site.

Topology

The topology to add an branch site with next generation firewall capabilities is shown in [Figure 3 on page 152](#).

Figure 3: Branch site with next generation firewall



Workflow

The following workflow describes the steps that are required to set up a firewall site and provision the firewall device associated with the site.

To set up a next generation firewall site and provision the firewall device:

1. Add a standalone next generation firewall site. See [“Add a Standalone Next-Generation Firewall Site” on page 153](#).

NOTE: Before proceeding to the next step ensure that the ZTP process is complete and the firewall device status is set to **Provisioned** state.

2. Configure the firewall device. See [“Configuring the Firewall Device” on page 303](#).
3. Add firewall policies for the site. See [“Adding a Firewall Policy” on page 445](#).
4. Add firewall policy intents for the firewall policies that you added. See [“Adding Firewall Policy Intents” on page 449](#).
5. Deploy firewall policies to the site. See [“Deploying Firewall Policies” on page 509](#).

Enabling Integration with Mist Access Points

You can enable integration with the Mist access points to easily access and view Mist access points connected to the branch network. When integration with Mist access point is enabled, the connected

access points are listed in the **Devices** tab of the **Resources > Site Management > Site Name** page. You can click the access point name to view the Mist access point details from the Mist portal that is integrated with CSO.

To enable integration with the Mist access point:

1. Select **Administration > WiFi Settings**.

The WiFi Settings page appears.

2. Click the Enable toggle button to enable integration with Mist access points.

The Login E-mail and Login Password fields appear.

3. In the Login E-mail page, enter the e-mail address that is the username for your Mist account.

4. In the Login Password page, enter the password for your Mist account.

5. Click **Save**.

After you enable integration and enter the login credentials, CSO adds the access point to the list of devices associated with a site. To view details about the access point, **Devices** tab of the **Resources > Site Management > Site Name** page and click the access point name. The Mist portal page for the selected device appears.

Add a Standalone Next-Generation Firewall Site

From CSO release 5.4.0 onward, the on-premises spoke (branch) site addition and site activation can be optionally separated, giving more flexibility to on-site installation of a CPE.

In SD-WAN deployments with next generation firewall (NGFW) capability comprising single or dual customer premises equipment (CPE), tenant administrators have an option to enter the serial number of the CPE device after adding the branch sites. The branch site can be added by a tenant administrator and activated manually by another authorized user. The authorized user must enter either the serial number and the activation code, or only the serial number when manually activating the CPE device later. The option to add branch sites without serial number of a CPE device is applicable to both SRX and NFX (NFX150 and NFX250) device templates.

You add the standalone NGFW site from the Site Management page.

To add a standalone NGFW site:

1. Select **Resources > Site Management**.

The Site Management page appears.

2. Click **Add** and select **Add Branch Site (Manual)**.

The Add Branch Site page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 29 on page 156](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **Next**.

A summary page is displayed.

5. Review the configuration and modify the settings, if needed, from the Summary tab. Click **OK**.

- If you entered a serial number during activation and automatic activation is enabled, the Site Activation Progress page appears. The site activation process proceeds through the tasks explained in *Troubleshooting Site Activation Issues*.

Click **OK** to close the Site Activation Progress page.

- If you did not enter a serial number and the automatic activation is disabled, you are returned to the Site Management page. CSO triggers a job and displays a confirmation message with a job link. Click the link to view the status of the job. After the job is finished, CSO displays a confirmation message with a job link. The status of the site changes to **CREATED**.

You must manually activate the device to finish the activation process.

NOTE: The following procedure is applicable if zero touch provisioning (ZTP) is set true in the device template. If ZTP is disabled in the device template, you must copy the stage-1 configuration and commit it on the device for CSO to proceed with the activation.

To manually activate the CPE (branch site) device:

- a. Select the branch site CPE that has to be activated.
- b. Click **Activate Site** link in the Site Management page.

The **Activate Site** page appears.

- c. Enter the serial number(s) of the device and the activation code. Click **OK**.

The **Site Activation Progress** page appears displaying the progress of steps executed for activating the CPE device. On successful activation of the device, the Site Status changes from **Created** to **Provisioned**.

- 6. If you have enabled the Zero Touch Provisioning field, CSO applies the stage-1 configuration automatically.

NOTE: The device is activated automatically, if you have already provided the activation code and device serial number while creating the firewall site.

If you have disabled the Zero Touch Provisioning field for the device, you must manually configure the stage-1 configuration on the device.

- a. Click the **Click to copy stage-1 config** link next to the Prestage Device task on the Site Activation Progress page. If you close the Site Activation Progress page inadvertently, you can access the page from the Site Management page. Click the **View** link next to the status of the site, under the Site Status column.

NOTE: You can also copy the configuration from the Devices page (Resources > Devices). Select the device and click **Stage1 Config**.

The Stage-1 Configuration page appears displaying the stage-1 configuration.

- b. Copy the stage-1 configuration.
- c. Log in to the device and enter Junos OS configuration mode.
- d. Paste the configuration that you copied and commit the configuration.

CSO applies the pre-script and stage-1 configuration (includes the device configuration). The status of the site changes to **MANAGED** on the Sites page.

If you selected Security Services while adding the device, then CSO generates the service provisioning configuration and applies it on the device. The firewall site status changes to **PROVISIONED** in the Site Management page.

If you did not select Security Services while adding the device, then the device remains in the **MANAGED** state until you apply the service. You can edit the site and add the service. After you add the service, CSO applies the service provisioning configuration and the device is provisioned.

NOTE: You can also add a standalone firewall site using the site templates. For more information, see [“Add Branch Sites by Using a Site Template” on page 220](#).

Table 29: Fields on the Add Branch Site Page (Standalone Firewall)

Field	Description
General	
Site Information	
Site Name	Enter a unique name for the firewall site. You can use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.
Device Host Name	The device host name is auto-generated and uses the format <i>tenant-name.host-name</i> . You cannot change the <i>tenant-name</i> part in the device host name. Use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.
Site Group	Select a site group to which you want to assign the site.
Site Capabilities	Select Security Services as you are adding a NGFW site. Note that Device Management is selected by default.
Address and Contact Information	
Street Address	Enter the street address of the site.
City	Enter the name of the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.

Table 29: Fields on the Add Branch Site Page (Standalone Firewall) (continued)

Field	Description
Country	<p>Select the country where the site is located.</p> <p>You can click the Validate button to verify the address that you specified:</p> <ul style="list-style-type: none"> • The address verification successful message is displayed if the address can be verified. You can click the View location on the map link to see the address location. • If the address cannot be verified, the Site address could not be validated message is displayed .
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
Advanced Configuration	
Domain Name Server (DNS)	Enter one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Enter the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers. Example: ntp.example.net The site must have DNS reachability to resolve the FQDN during site configuration.
Select Timezone	Select the time zone for the site.
Device	
Device Redundancy	Disabled by default. Enable this option only for dual CPEs.
Device Series	SRX is displayed by default.
Device Model	Select the device model.
Device Root Password	The default root password is fetched from the ENC_ROOT_PASSWORD field in the device template. You can retain the password or change it by entering a password in plain-text format. The password is encrypted and stored on the device.

Table 29: Fields on the Add Branch Site Page (Standalone Firewall) (continued)

Field	Description
Serial Number	<p>Enter the serial number of the firewall device. Note that the serial numbers are case-sensitive.</p> <p>If you do not enter the serial number, the branch site is created but the CPE device is not activated. See “Step-by-Step Procedure” on page 78 for more information.</p>
Zero Touch Provisioning	<p>Click the toggle button to enable or disable Zero Touch Provisioning (ZTP). This option is enabled by default.</p> <p>To use ZTP, ensure the following:</p> <ul style="list-style-type: none"> Device must have connectivity to CSO and Juniper phone-home server (https://redirect.juniper.net) Use telnet to verify connectivity: telnet redirect.juniper.net:443 telnet CSO Hostname/IP:443 If the connection is established, the device has connectivity to the phone-home server and CSO. Required certificates for phone-home server and CSO must be present on the device. <p>If ZTP is enabled, the Boot Image field is displayed and you must select an image that supports the Phone-Home client. During ZTP, the image on the firewall device is upgraded to the image that you select for the Boot Image.</p> <p>If you disable ZTP, ensure that the device has connectivity to CSO. If the device is not prestaged/preconfigured, then you must provide the details under the Management Connectivity section so that CSO can generate the configuration as part of the stage-1 configuration. You can skip the Management Connectivity section if the device has connectivity to CSO.</p> <p>If you disable ZTP, you must copy the stage-1 configuration from CSO and commit it on the device to start the onboarding process. Use any of the following options to copy the stage-1 configuration:</p> <ul style="list-style-type: none"> Click the Click to copy stage-1 config link next to Prestage Device task on the Site Activation Progress page. If you close the Site Activation Progress page inadvertently, you can access the page from the Site Management page. Click the View link next to the status of the site under the Site Status column. On the Devices page (Resources > Devices), select the device and click Stage1 Config.

Table 29: Fields on the Add Branch Site Page (Standalone Firewall) (continued)

Field	Description
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the device. This option is enabled by default.</p> <p>If you disable automatic activation, refer “Activate a Device” on page 252 topic to manually activate the CPE.</p>
Activation Code	If the automatic activation of the device is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.
Management Interface Family	Select the IP address type (IPv4 or IPv6) for the management interface. This field is displayed only if you have enabled Zero Touch Provisioning .
Boot Image	<p>When the Zero Touch Provisioning field is enabled, select the boot image from the drop-down list to upgrade the image on the firewall device to a version that supports the phone-home client.</p> <p>The boot image is the device image that was previously uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process. If the boot image is not provided, then the device skips the automatic upgrade procedure. The boot image is populated based on the device template that you have selected while creating a site.</p> <p>By default, the Use Image on Device option is selected.</p>
Device Information	
Secure Log Source Interface	Select the port that you want to configure as management interface and connect it to the management device. You can configure any of the ge-0/0/x ports, where x ranges from 0 to 14, as in-band management interfaces.
Firewall Policies	<p>This field is displayed only if you enable Zero Touch Provisioning. Select the firewall policy that you want to deploy to the standalone firewall site. The firewall policy list is populated from the Configuration > Firewall > Firewall Policy page.</p> <p>Default: Factory_Default_Fw_Policy</p>
NAT Policies	<p>This field is displayed only if you enable Zero Touch Provisioning. Select the NAT policy that you want to deploy to the standalone firewall site. The NAT policy list is populated from the Configuration > NAT > NAT Policies page.</p> <p>Default: Factory_Default_NAT_Policy</p>

Table 29: Fields on the Add Branch Site Page (Standalone Firewall) (continued)

Field	Description
Import Policy Configuration	<p>This field is displayed only if you disable Zero Touch Provisioning.</p> <p>By default, this field is disabled. Click the toggle button to automatically import firewall policies and NAT policies from a NGFW device to CSO.</p> <p>The following are the firewall and NAT configurations that are imported for this site:</p> <p>Firewall rules (zone rules):</p> <ul style="list-style-type: none"> • Address objects (address group or address object) • Service objects (custom service) • Custom L7 applications or application groups • SSL/UTM profiles and schedulers • Users (UserFW) <p>NAT rules (Source/Destination/Static):</p> <ul style="list-style-type: none"> • NAT pools
Management Connectivity	
NOTE: This section is displayed only if you disable Zero Touch Provisioning.	
Address Family	Select the IP address type (IPv4 or IPv6).
Interface Name	Enter the management interface.
Access Type	Select the access type for the underlay link. LTE, ADSL, and VDSL access types are supported only on Internet links. You cannot add LTE, ADSL, and VDSL access types to the same WAN link.
Address assignment	By default, DHCP is selected. If you want to provide a static IP address, select STATIC.
Management VLAN ID	Enter a VLAN ID for the WAN link.
PPPoE	Click the toggle button to enable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet).
Configuration Templates (Optional)	

Table 29: Fields on the Add Branch Site Page (Standalone Firewall) (continued)

Field	Description
Configuration Templates List	<p>(Optional) Select one or more configuration templates from the list. This list is filtered based on the device that you select.</p> <p>Configuration templates are stage-2 templates that are added by your OpCo administrators or SP administrators or Tenant administrators.</p> <p>To set the parameters for the selected configuration templates:</p> <ol style="list-style-type: none"> 1. After you select one or more configuration templates, click Set Parameters. The Device Configurations page appears. This page consists of two tabs—CONFIGURATION and SUMMARY. 2. In the CONFIGURATION tab fill in the attributes for each of the configuration templates. (Optional) View the CLI commands in the Summary tab. 3. Click Save. You have added and set the parameters for the configuration templates that are part of the site template that you are creating.

RELATED DOCUMENTATION

| [Adding and Provisioning a Next Generation Firewall Overview](#) | 151

Managing LAN Segments on a Tenant Site

IN THIS SECTION

- [Adding LAN Segments](#) | 162
- [Edit a LAN segment](#) | 168
- [Deploying LAN Segments](#) | 169
- [Deleting LAN Segments](#) | 170

A network on a tenant site is divided into multiple LAN segments to improve traffic management and security. A LAN segment is a small portion of a LAN that is used by a work group. A grouping of multiple LAN segments form a department. LAN segments are separated by a bridge or router.

Starting from Release 6.1.0, CSO supports automatic discovery of subnets behind LAN routers, which are connected to a Customer Premise Equipment (CPE) such as NFX or SRX Series devices. Administrators can announce additional subnets on a LAN segment by using static and dynamic routing.

In addition, CSO enables you to control the route advertisements per LAN segment.

You can view and manage LAN segments from the LAN tab of the *Site Name* page.

These topics describe how to manage LAN segments on a site.

Adding LAN Segments

You add LAN segments from the *Site Name* page.

To add a LAN segment:

1. Click **Resources > Site Management**.

The Sites page appears.

2. Click the site for which you want to add the LAN segment.

The *Site-Name* page appears.

3. Click the add icon (+) on the **LAN** tab.

The Add LAN Segment page appears.

4. Complete the configuration settings according to the guidelines provided in [Table 30 on page 163](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

5. Click **OK**.

You are returned to the *Site-Name* page, where the LAN segment that you added is displayed.

Table 30: Add LAN Segment Settings

Field	Description
Use for Overlay VPN	<p>Enable the Use for Overlay VPN field to associate the LAN segment with the selected department (VRF + ZONE) for overlay traffic to other sites.</p> <p>Disable the Use for Overlay VPN field to associate the LAN segment with a security zone for underlay breakout. You must define zone-based security policies.</p> <p>NOTE: When adding a new site, this field is enabled by default and cannot be modified. However, when you add a new LAN Segment to a provisioned site from the LAN tab of the Site-Name page, you can enable or disable this option.</p>
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length allowed is 15 characters.</p>
CPE Port	<p>NOTE: Applicable to SRX Series devices.</p> <p>Select the CPE port to be added in the LAN segment.</p> <p>When you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page, you can select (or create) a LAG interface or a redundant Ethernet (reth) interface (for dual CPE cluster) to connect the SRX Series CPE devices to an EX series switch.</p> <p>To use the et interface on SRX4600 devices, you must create a LAG interface and configure the et interface as a member of the LAG (aggregated Ethernet or ae) interface. See “Create LAG Interface” on page 312.</p> <p>For an SRX4600 dual CPE cluster, you can use the et interface if it is configured as a member of the redundant Ethernet (reth) interface.</p>
Add LAG Interface	<p>NOTE: This option is available when you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page.</p> <p>Click the link to create a LAG interface (ae interface) if you want to use it to connect the SRX Series CPE to the EX Series switch. See “Create LAG Interface” on page 312 for details.</p>
Create RETH Interface	<p>NOTE: This option is available when you add a new LAN Segment to a provisioned site from the LAN tab of the <i>Site-Name</i> page.</p> <p>Click the link to create a reth interface for an SD-WAN site with a dual CPE cluster. See “Create a RETH Interface” on page 314 for details.</p>

Table 30: Add LAN Segment Settings (*continued*)

Field	Description
Type NOTE: This field is displayed only for LAN segments associated with enterprise hub sites.	Select the type of LAN segment: <ul style="list-style-type: none"> • Directly Connected (default)—Indicates that the LAN segment is directly connected to the site. • Dynamic Routed—Indicates that the LAN segment is not directly connected to the site and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.
VLAN ID	Enter the VLAN ID for the LAN segment. By default, VLAN ID is set to 1 and native VLAN is enabled for untagged traffic. Range: 1 to 4049 .
Use for Native VLAN	Enable this option to use the VLAN ID specified above for untagged traffic. The CPE interface is configured with a native-vlan-id, which has the same value as the VLAN ID.
Department	NOTE: This field is available only if the Use for Overlay VPN field is enabled. Select a department to which the LAN segment is assigned. Alternatively, click the Create Department link to create a new department and assign the LAN segment to it. See “Add a Department” on page 783 for details. You can group LAN segments as departments for ease of management and for applying policies at the department-level. For LAN segments that are dynamically routed, you can assign only a data center department.
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment. This address will be the default gateway for endpoints in this LAN segment. For example: 192.0.2.8/24.
Zone	NOTE: This field is available only if the Use for Overlay VPN field is disabled. Select a security zone to be associated with this LAN segment. Alternatively click Create Zone to create a new security zone and assign that to this LAN segment. See “Adding a Security Zone” on page 318 for details.
DHCP	For directly connected LAN segments, click the toggle button to enable DHCP. You can enable DHCP if you want to assign IP addresses by using a DHCP server or disable DHCP if you want to assign a static IP address to the LAN segment. NOTE: If you enable DHCP, additional fields appear on the page.

Table 30: Add LAN Segment Settings (*continued*)

Field	Description
Additional fields related to DHCP	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server. Default: 1440 Range: 0 through 4,294,967,295 seconds.
Name Server	Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address. NOTE: DNS servers are used to resolve hostnames into IP addresses.
CPE Ports	NOTE: Applicable to NFX150 and NFX250 devices. For sites with SD-WAN capability, the CPE Ports field is disabled and the CPE ports that you can include in the LAN segment are listed. Select the ports from the Available column and click the right-arrow to move the ports to the Selected column.
Static Routing	
Use this section to configure static routing on the LAN segment. Provide the IP addresses of all the LAN routers connected to the CPE device and the static subnets behind these routers.	
<i>Add LAN Router IP Prefix</i>	
LAN Router IP	Enter the IP address of the LAN router that is connected to the CPE device.
Prefix	Enter the subnets that are connected to the LAN router.
BFD	Enable Bidirectional Forwarding Detection (BFD) to detect any failures on the static route.

Table 30: Add LAN Segment Settings (*continued*)

Field	Description
<i>Dynamic Routing</i>	
Routing Protocol	Enable this toggle button to configure dynamic routing using the BGP or OSPF protocol.
BFD	Enable Bidirectional Forwarding Detection (BFD) to detect any failures in the LAN segment.
Protocol	Select either BGP or OSPF.
BGP Configuration	
<p>NOTE: Starting in Release 6.1.0, CSO explicitly disables the long-lived graceful restart (LLGR) capability for BGP peering sessions with provider edge (PE) and data center or LAN routers. Disabling LLGR ensures that the CPE does not differentiate the route advertisements to the peering router irrespective of the peering router's LLGR capability.</p> <p>Prior to CSO Release 6.1.0, LLGR helper mode is enabled by default (implicit behavior of Junos OS) on the CPE for BGP peering towards PE router in IP VPN deployments, and data center or LAN routers in data center deployments.</p>	
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> • None—Indicates that no authentication should be used. This is the default. • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.
BGP Options	<p>You can select the following options based on your requirements:</p> <ul style="list-style-type: none"> • AS-OVERRIDE: Replaces all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer. • AS-PATH-PREPEND: Prepends one or more autonomous system (AS) numbers at the beginning of an AS path. Prepending an AS path makes a shorter AS path look longer and therefore it becomes less preferable to BGP. • AS-LOOP: Allows the local device's AS number to be added in the received AS paths. You can specify the number of times the detection of local AS is allowed in the AS path.
Loop Count	<p>This field is displayed only if you select AS-LOOP.</p> <p>Enter the maximum number of times the detection of local AS is allowed in the AS path.</p>

Table 30: Add LAN Segment Settings (*continued*)

Field	Description
Peer IP Address	Enter the IP address of the LAN BGP peer.
Peer AS Number	Enter the autonomous system (AS) number of the LAN BGP peer. By default, CSO uses the AS number 64512. You can enter a different AS number.
Local AS Number	Enter the local AS number. When you configure this parameter, the local AS number is used for BGP peering instead of the global AS number configured for the CPE.
<i>OSPF Configuration</i>	
OSPF Area ID	Specify the OSPF area identifier to be used for the dynamic route.
Authentication	<p>Select the OSPF route authentication method to be used:</p> <ul style="list-style-type: none"> • Password—Indicates that password-based authentication should be used. If you choose this option, you must specify the password. (This is the default). • Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key. • None—Indicates that no authentication should be used.
Password	Enter the password to be used to verify the authenticity of OSPF packets.
Confirm Password	Retype the password for confirmation purposes.
MD5 Auth Key ID	<p>If you specified that MD5 should be used for authentication, enter the OSPF MD5 authentication key ID.</p> <p>Range: 1 through 255.</p>
Auth Key	If you specified that MD5 should be used for authentication, enter an MD5 authentication key, which is used to verify the authenticity of OSPF packets.
<i>Route Advertisement Control</i>	
LAN Route(s) to Overlay	When this option is enabled, LAN routes are advertised to the remote CPEs. By default, this option is enabled.

Table 30: Add LAN Segment Settings (*continued*)

Field	Description
Overlay Route(s) to LAN	<p>This option is displayed only if you enable the Routing Protocol toggle button. By default, this option is disabled.</p> <p>Enable this option to advertise the remote CPE routes received in a department to the LAN router.</p> <p>NOTE: In CSO Release 6.0.0 and earlier releases, this option is called Advertise LAN Prefix and is applicable only for data center departments.</p>
Static/Aggr Routes to Overlay	<p>Enable this option to allow advertisement of static or aggregate routes to the overlay network.</p> <ul style="list-style-type: none"> • If a large number of LAN routes are present, then you can disable the LAN Route(s) to Overlay option and use this option to advertise aggregate routes. • If you want to advertise additional routes, then you can enable the LAN Route(s) to Overlay option and use this option to advertise additional static routes.

Edit a LAN segment

You can edit LAN segments associated with a site from the LAN tab in the Site Management page.

To edit a LAN segment:

1. Click **Resources > Site Management**.

The Site Management page appears.

2. Click the *Site-Name* link for which you want to edit the associated LAN segment.

The *Site-Name* page appears.

3. Select the **LAN** tab.

The associated LAN segments are displayed.

4. Select the LAN segment you want to edit and click the **edit** (pencil) icon.

The Edit LAN segment page appears.

5. Complete the configuration settings according to the guidelines provided in [“Add LAN Segment Settings” on page 163](#).

NOTE: You cannot edit the **Name** and **Use for Overlay VPN** fields.

6. Click **OK**.

An Edit LAN segment job is triggered and you are returned to the LAN tab of the Site Management page.

A confirmation message appears (with the job link) at the top of the page indicating that the job was created. You can click the job link to view details of the job (including job status, start date and time, and end date and time). Alternatively, you can view the status of the job on the Jobs (**Monitor > Jobs**) page.

After the Edit LAN segment job is completed successfully, the edited LAN segment with status as **Modified** is listed on the LAN tab of the Site Management page.

7. Deploy the modified LAN segment to apply the changes on the site. See [“Deploying LAN Segments” on page 169](#).

Deploying LAN Segments

After you create a LAN segment and assign it to a department, you must deploy the LAN segment. You can deploy LAN segments from the *Site Name* page.

To deploy one or more LAN segments:

1. Click the **LAN** tab.
2. Select one or more LAN segments that you want to deploy and click **Deploy**.

A Deploy LAN Segment job is created.

NOTE: If a Deploy LAN Segment job is in progress for a site, wait for the job to finish before triggering another Deploy LAN Segment job.

If you attempt to trigger a Deploy LAN segment job when another one is running, the job fails with a message indicating that the previous LAN segment deployment job is in progress.

3. Click **More > Deploy History** to view job status and deployment history of the LAN segment.

The **Deploy LAN Segment History** page displayed.

Alternatively, you can verify the status of the job from the **Monitor > Jobs** page.

Deleting LAN Segments

You can delete a LAN segments from the *Site Name* page.

To delete a LAN segment:

1. Select a LAN segment and click the delete icon (X) icon on the **LAN** tab.

The Delete LAN Segment page appears.

2. Click **OK** to confirm deletion.

The LAN segment is deleted.

Manage a Site

Tenant administrator users can use the *Site-Name* page to view the details of a site and manage configurations of the site.

To view the details of a site or manage the site:

1. Click **Resources > Site Management**.

The Site Management page appears.

2. Click the *Site-Name* link of the site that you want to manage.

The *Site-Name* page appears.

On the *Site-Name* page, depending on the type of site or the service selected for the site, one or more of the following tabs are displayed:

- **Overview** tab:

View general information about the site and the devices associated with the site. You can also view information about the recent alarms and alerts generated in the site. See [Table 31 on page 173](#).

- **IPVPN** tab:

View and configure IP VPN (Layer 3) parameters to connect an existing Layer 3 VPN to a network managed by Contrail Service Orchestration (CSO) through a provider hub site. For more information on IP VPN parameters, see [Table 32 on page 174](#).

You can add, edit, or delete IP VPN configuration for a provider hub site. For more information, see [“Add IP VPN Configuration to Provider Hubs” on page 182](#), [“Edit IP VPN Configuration for Provider Hubs” on page 185](#), and [“Delete IP VPN Configuration from Provider Hubs” on page 186](#).

NOTE:

- IP VPN can be configured only for provisioned provider hub sites with OAM_AND_DATA or DATA_ONLY capability for each tenant department VPN.
- IP VPN configuration is not applicable for data center department VPNs.

- **WAN tab:**

View detailed information about the WAN links of the site. You can also add or delete a mesh tunnel between a source site and a destination site. See [Table 33 on page 175](#).

NOTE: This tab is available only for SD-WAN sites.

- **Policies tab:**

View the list of policies applied to a site (Firewall, NAT, SSL proxy, or SD-WAN policy). Click the policy name to view the rules or intents that are applied to the site.

You can also view:

- The name of the tenant user who last updated the policy.
- The date and time at which the policy was updated.
- Deployment status of the policy (deployed or undeployed).

NOTE: This tab is available for SD-WAN and NGFW sites.

To edit a policy, click the edit icon (at the end of the row) and you are taken to:

- Firewall Policy page (**Configuration > Firewall > Firewall Policy**) to edit firewall policies.

For more information, see [“Editing and Deleting Firewall Policies” on page 447](#).

- NAT Policies page (**Configuration > NAT > NAT Policies**) to edit NAT policies.

For more information, see [“Editing and Deleting NAT Policies” on page 635](#).

- SSL Proxy Policy page (**Configuration > SSL Proxy > Policy**) to edit SSL proxy policies.

For more information, see [“Editing, Cloning, and Deleting SSL Proxy Policy Intents” on page 722](#).

- SD-WAN Policy page (**Configuration > SD-WAN > SD-WAN Policy**) to edit SD-WAN policies.

For more information, see [“Editing and Deleting SD-WAN Policy Intents” on page 583](#).

- **Devices tab:**

View, manage, and delete the devices for the site.

You can also:

- Push licenses to a device
- Activate a device
- View and deploy stage-1 configuration to a device
- Download the cloud info template

For more information on the fields displayed and tasks you can perform on the Devices tab, see [“About the Devices Page” on page 271](#) and [“Activate a Device” on page 252](#).

- **LAN tab:**

View, create, edit, deploy, and delete a LAN segment. For information on the fields displayed, see [“Adding LAN Segments” on page 162](#).

Additionally, you can:

- Reassign a LAN segment to a different department.
- View the devices in a LAN segment and deploy any of these devices.
- View the status of the deployment.

For more information on the fields displayed and tasks you can perform on the LAN tab, see [“Managing LAN Segments on a Tenant Site” on page 161](#).

- **Services tab:**

View the network services allocated to the tenant.

Additionally, you can:

- Deploy network services to a site: Select the network service, and then select an attachment point in the topology graphic. Alternatively, you can drag and drop the network service to an attachment point in the topology graphic.
- Start a network service. For more information, see [“Start a Network Service” on page 178](#).
- Disable a network service. For more information, see [“Disable a Network Service” on page 180](#).
- Delete a network service. For more information, see [“Delete a Network Service” on page 181](#).

NOTE: This tab is available only for SD-WAN sites.

[Table 31 on page 173](#) describes the widgets displayed on the Overview tab of the *Site-Name* page.

Table 31: Widgets on the Overview tab

Widget	Description
General Info	<p>View the following general information about the site:</p> <ul style="list-style-type: none"> • Tenant name • Site Type (branch, enterprise hub, provider hub, or cloud spoke) • Site Role (spoke or hub) • Geographical location of the site • Contact information of the tenant • VPN Authentication Type (using preshared key or public key infrastructure [PKI] certificate) • Encryption Type (By default, it is AES-256-GCM. See <i>Encryption Type</i> in “View and Edit Tenant Settings” on page 27.)
Recent Alarms	<p>View the recent critical, major, and minor alarms generated in the site with the date and time of occurrence.</p> <p>From the Period list, you can select one of the following values to filter the generated alarms based on their time of occurrence:</p> <ul style="list-style-type: none"> • Previous one hour • Previous eight hours • Previous one day • Previous one week • Previous one month <p>You can click View All Alarms at the bottom-right corner of the Recent Alarms widget to view all the generated alarms in the Alarms page (Monitor > Alerts & Alarms > Alarms). For more information, see “About the Alarms Page” on page 817.</p>

Table 31: Widgets on the Overview tab (continued)

Widget	Description
Recent Alerts	<p>View the recent critical, major, and minor alerts generated in the site with the date and time of occurrence.</p> <p>From the Period list, you can select one of the following values to filter the generated alerts based on their time of occurrence:</p> <ul style="list-style-type: none"> • Previous one hour • Previous eight hours • Previous one day • Previous one week • Previous one month <p>You can click View All Alerts at the bottom-right corner of the Recent Alerts widget to view all the generated alerts in the Alerts page (Monitor > Alerts & Alarms > Alerts). For more information, see “About the Generated Alerts Page” on page 810.</p>
Connectivity & Devices	<p>View the following general information about all the provisioned devices in the site:</p> <ul style="list-style-type: none"> • Device Name • Device Model • Device Serial Number • Device Status

Table 32: Fields on the IPVPN tab for provider hubs

Field	Description
Department VPN	Name of the department VPN associated with the IP VPN configuration.
Interface Name	Enter the name of the physical interface on which you want to enable eBGP between provider hub site and the PE router.
VLAN ID	<p>VLAN ID of the interface.</p> <p>Range: 1 through 4094.</p>
Interface IP Prefix	IPv4 address with a prefix of the interface.

Table 32: Fields on the IPVPN tab for provider hubs (*continued*)

Field	Description
AS Loop Count	<p>Maximum number of times the detection of local Autonomous System (AS) number is allowed in the AS path. If this count exceeds the specified AS loop count, the system discards this route. This helps in preventing routing loops. For example, if you configure AS Loop Count as 1, the route is discarded if the neighbor's local AS is detected in the path more than once.</p> <p>Range: 1 through 10.</p>
eBGP Peer-AS-Number	<p>Autonomous system (AS) number for the eBGP peer.</p> <p>Range: 1 through 4294967295.</p>
Neighbor Address	IPv4 address of the peer interface.
Status	Status of the IP VPN configuration (in progress or deployed).

[Table 33 on page 175](#) describes the widgets displayed on the WAN tab of the *Site-Name* page.

Table 33: Widgets on the WAN tab (Overlay and Underlay)

Widget	Description
Overlay and Underlay topology of WAN links	<p>Displays the WAN link topology of the site.</p> <p>Links displayed in green are up (active) and red are down.</p> <p>For all sites in full mesh topology, you can view all the connected WAN interfaces for each site. Click the site connection point to see all connections between its WAN interfaces. You can view general information about each WAN interface when you hover over it.</p>
Overlay WAN Widgets	

Table 33: Widgets on the WAN tab (Overlay and Underlay) (continued)

Widget	Description
Time Range	<p>Select the time range by clicking on one of the following options:</p> <ul style="list-style-type: none"> • 2 hours (2h) • 4 hours (4h) • 8 hours (8h) • 16 hours (16h) • 24 hours (24h) • 1 week (1w) <p>You can select a custom time range by clicking Custom and selecting the To and From timing. You can also drag the Time Range slider (from either sides) to select a custom time range.</p> <p>NOTE: All the information displayed on this tab is updated based on the time range you select.</p>
Overall Network Statistics	<p>Displays the following metrics for the selected WAN interface in the selected timeframe:</p> <ul style="list-style-type: none"> • Number of active dynamic VPN (DVPN) tunnels • Throughput (in bps) • Latency (in ms) • Packet loss (in percentage) • E2E (end-to-end) delay (in ms) • Jitter (in ms) • Total bytes transmitted and received
Link Metrics	<p>Displays a graphical representation of traffic on each WAN link for the selected time interval. You can update the graph based on any of following filters (drop-down list):</p> <ul style="list-style-type: none"> • Site Traffic: Total bytes, Transmitted bytes, Received bytes, or Throughput (in bps) • Events: SLA not met, Switch events, or None • Profiles (SLA based steering profiles): CSO-AV, CSO-Sec, CSO-Email, CSO-Productive, or CSO-FileShare.
Top Applications	<p>Displays a horizontal bar chart of the top applications that generate the maximum traffic in the spoke site or enterprise hub site.</p> <p>You can select the Site traffic list to update the chart based on the total bytes, transmitted bytes, received bytes, or throughput (in bps).</p>

Table 33: Widgets on the WAN tab (Overlay and Underlay) (continued)

Widget	Description
Link Utilization	<p>Displays the link utilization (in percentage) as a circular chart of the top 10 applications and other applications. You can also view the total link capacity consumed (in bytes). You can select the Site traffic list to update the chart based on total bytes, transmitted bytes, received bytes, or throughput (in bps).</p>
On-Demand VPN Threshold Details	<p>When you hover over On-Demand VPN Threshold Details, you can view the threshold for creating and deleting tunnels, device SKU, maximum number of tunnels allowed, and minimum number of tunnels required before deactivation.</p> <p>Additionally, you can:</p> <ul style="list-style-type: none"> • Add or delete dynamic mesh tunnels between a source site and a destination site. See “Adding On-Demand Mesh Tunnels” on page 244 or “Deleting On-Demand Mesh Tunnels” on page 246. • Reconfigure static tunnels for a branch site or an enterprise hub site. See <i>Reconfigure Static Tunnels</i>. <p>You also can view the following details of the dynamic mesh tunnels history for the selected site:</p> <p>NOTE: A new row is added to this table when there is a change in the tunnels associated with the particular site and the table entries are grouped by the destination site.</p> <ul style="list-style-type: none"> • Type of tunnel (DVPN or Static) • Operation (create, update, or delete tunnel) performed on the site • Time (date and time at which the operation was completed) • Reason for performing the operation. It can be one the following: <ul style="list-style-type: none"> • ZTP: Static tunnels were added during ZTP. • Traffic: Tunnels were added or deleted based on the site traffic (after crossing the configured on-demand VPN threshold value). • Admin: You manually add, update, or delete the tunnels. • RMA: Based on the Return Material Authorization (RMA) performed on a site, the on-demand tunnels are created or deleted. • No. of overlay WAN links between two sites (branch sites or enterprise hub sites) on which the operation was performed. <p>NOTE: A maximum of four links are allowed between two sites.</p>

Underlay WAN Widgets

Table 33: Widgets on the WAN tab (Overlay and Underlay) (continued)

Widget	Description
WAN Link Throughput Over Time	<p>Displays a line chart of WAN interface utilization as throughput (in bps) over time for each underlay WAN link. Different color lines represent the input and output rate for each WAN link. You can select them by hovering over the input/output rate list on the right side of the widget. Every three minutes the bandwidth usage information is collected for each WAN link and the rate is displayed respectively on the graph.</p> <p>You can view the utilization statistics for a particular time range by selecting any one of the following values from the Time Span list:</p> <ul style="list-style-type: none"> • Last 15 min • Last 30 min • Last 1 hour • Last 8 hour • Last 1 day • Last 1 week • Last 1 month <p>NOTE: You must upgrade the site to CSO Release 6.0.0 to view this widget. For more information, “Upgrading Sites” on page 211.</p>

RELATED DOCUMENTATION

[About the Site Management Page | 68](#)
[Dynamic Mesh Tunnels Overview | 243](#)

Start a Network Service

You can start or instantiate a network service for a site from the *Site-Name* page in Customer Portal.

NOTE: Ensure that the Service Provider (SP) or Operating company (OpCo) administrator user allocates at least one network service to you from the Administration Portal.

To instantiate a network service:

1. Click **Resources > Site Management**.

The Site Management Page appears.

2. Click the *Site-Name* link for which you want to instantiate a network service.

The *Site-Name* page appears.

3. Select the **Services** tab.

The Services topology graphic appears. The Deploy Network Services pane appears on the right listing all the available network services for the site.

NOTE: When you select a network service, on the Deploy Network Services pane, you can view the network service description, service type, version, and timestamp of its last update.

4. Do one the following:

- Select a network service from the Deploy Network Services pane. On selecting the service, the eligible attachment points are highlighted in green on the topology graphic. Select the required attachment point.
- Drag and drop the network service you want to instantiate, from the Deploy Network Services pane to the attachment point on the topology graphic.

The Configure Network Service page appears.

5. Configure the parameters displayed based on the type of network service selected.

6. Click **OK**.

A confirmation message is displayed stating that the operation was successful and the topology graphic is updated with the selected network service.

7. Click **Start Service**.

A confirmation message appears stating that the network service is successfully instantiated and you are returned to the Services page.

The attachment point you selected on the topology graphic is updated with the instantiated network service.

RELATED DOCUMENTATION

[Network Service Overview](#) | 745

Disable a Network Service

You can disable a network service associated with a site from the *Site-Name* page in Customer Portal.

NOTE: Ensure that:

- The Service Provider (SP) or Operating company (OpCo) administrator user allocates at least one network service to you from the Administration Portal.
- You instantiate at least one network service on the *Site-Name* page in Customer Portal.

To disable a network service:

1. Click **Resources > Site Management**.

The Site Management Page appears.

2. Click the *Site-Name* link for which you want to instantiate a network service.

The *Site-Name* page appears.

3. Select the **Services** tab.

The Services topology graphic appears.

4. On the topology graphic, select the service which is currently instantiated.

5. Click **Disable Service**.

A confirmation message appears stating that the network service is successfully disabled and you are returned to the Services page.

The network service is disabled on the topology graphic.

RELATED DOCUMENTATION

[Network Service Overview](#) | 745

Delete a Network Service

You can delete a network service associated with a site from the *Site-Name* page in Customer Portal.

NOTE: You must disable the network service before deleting it. For more information, see [“Disable a Network Service” on page 180](#).

To delete a network service:

1. Click **Resources > Site Management**.

The Site Management page appears.

2. Click the *Site-Name* link for which you want to delete the network service.

The *Site-Name* page appears.

3. Select the **Services** tab.

The Services topology graphic appears.

4. Select the network service on the topology graphic.

5. Click **Disable Service**.

6. Click the **Delete** icon (trash can).

A confirmation dialog box appears.

7. Click **Yes**.

The network service is removed from the topology graphic and you are returned to the Services page.

RELATED DOCUMENTATION

[Network Service Overview](#) | 745

Add IP VPN Configuration to Provider Hubs

You can configure IP VPN (Layer 3) parameters to connect an existing Layer 3 VPN which is not managed by Contrail Service Orchestration (CSO) to a network managed by CSO through a provisioned provider hub site.

Figure 4: IP VPN sample topology

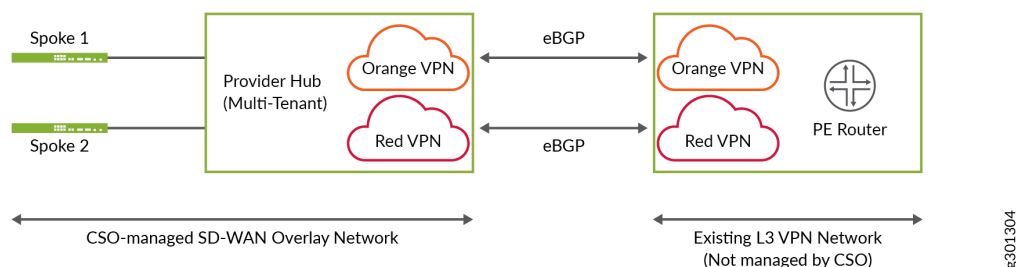


Figure 4 on page 182 shows a sample network topology with IP VPN interconnect. On the left side, a CSO-managed SD-WAN overlay network is shown consisting of a multi-tenant provider hub which can be connected to multiple spoke sites or enterprise hub sites belonging to different tenants. On the right side, an existing L3 VPN network which is not managed by CSO is shown. The PE router interconnects with the provider hub to create an IP VPN. Two departmental VPNs, orange and red, connects the provider hub and the PE router using point-to-point external BGP (eBGP) peering. This peering is implemented using Inter-AS Option-A. For more information, see [Interprovider VPNs](#).

NOTE:

- IP VPN can be configured only for provisioned provider hub sites with OAM_AND_DATA or DATA_ONLY capability for each tenant department VPN.
- IP VPN configuration is not applicable for data center department VPNs.
- Starting in Release 6.1.0, CSO explicitly disables the long-lived graceful restart (LLGR) capability for BGP peering sessions with provider edge (PE) and data center or LAN routers. Disabling LLGR ensures that the CPE does not differentiate the route advertisements to the peering router irrespective of the peering router's LLGR capability.

Prior to CSO Release 6.1.0, LLGR helper mode is enabled by default (implicit behavior of Junos OS) on the CPE for BGP peering towards the PE router in IP VPN deployments, and data center or LAN routers in data center deployments.

To add an IP VPN configuration:

1. Click **Resources > Site Management**.

The Site Management page appears.

2. Click the *Provider-Hub-Name* link to which you want to add an IP VPN.

The *Site-Name* page appears.

3. Click the **IPVPN** tab.

4. Click the **Add** icon (+).

The Add IPVPN Configuration page appears.

5. In the **Department VPN(s)** field, select one or more VPNs listed on the left column and click the right arrow (>) icon.

NOTE:

- The VPNs associated with standard departments are listed here. For more information, see [“About the Departments Page” on page 781](#).
- For tenants with network segmentation disabled, a single VPN shared by all its departments is displayed.

6. Click **Next** and complete the configuration as per the guidelines in [Table 34 on page 184](#), or click **Previous** to make changes on the previous page.

NOTE:

- If you select more than one VPN, you must configure the IP VPN parameters for each VPN separately on the **Configure IPVPN** page as per the guidelines in [Table 34 on page 184](#).
- Fields marked with an asterisk (*) are mandatory.

7. Click **Finish**.

A Configure IPVPN job is triggered and you are returned to the IPVPN page.

A confirmation message appears (with the job link) at the top of the page indicating that the job was created. You can click the job link to view the status of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page.

Table 34: Fields on the Add IPVPN configuration page

Field	Description
Interface Name	Enter the name of the physical interface on which you want to enable external BGP (eBGP) between provider hub site and the PE router. For example, ge-0/0/10.
VLAN ID	Enter the VLAN ID of the interface. Range: 1 through 4094.
Interface IP Prefix	Enter IPv4 address with a prefix for the interface. For example, 10.10.10.1/24.
AS Loop Count	Enter the maximum number of times the detection of local Autonomous System (AS) number is allowed in the AS path. If this count exceeds the specified AS loop count, the system discards this route. This helps in preventing routing loops. For example, if you configure AS Loop Count as 1, the route is discarded if the neighbor's local AS is detected in the path more than once. Range: 1 through 10.
eBGP Peer-AS-Number	Enter the autonomous system (AS) number for the eBGP peer. Range: 1 through 4294967295.
Neighbor Address	Enter the IPv4 address of the peer interface.
Local AS number	Enter the local AS number for the IP VPN configuration. When you configure this parameter, the local AS number is used for eBGP peering instead of the global AS number configured for the provider hub.
Authentication	Select one of the following BGP route authentication method: <ul style="list-style-type: none"> • None: Indicates that no authentication should be used. This is the default. • Use MD5: Indicates that MD5 is to be used for authentication. If you choose this option, specify an MD5 authentication key (password), which is used to verify the authenticity of the BGP packets.
Disable Graceful Restart	Disable graceful restart configuration for the provider hub by clicking the toggle button while trying to peer with a device which does not have the graceful restart capability. By default, graceful restart helper mode, the ability to assist a neighboring router attempting a graceful restart, is enabled.

RELATED DOCUMENTATION

About the Site Management Page | 68

Manage a Site | 170

About the Departments Page | 781

Edit IP VPN Configuration for Provider Hubs

To edit an IP VPN configuration:

1. Click **Resources > Site Management**.

The Site Management page appears.

2. Click the provider hub *Site-Name* link to edit an associated IP VPN.

The *Site-Name* page appears.

3. Select the **IPVPN** tab.

4. Select the department VPN whose configuration you want to edit.

5. Click the **Edit** icon (pencil).

The Edit IPVPN Configuration page appears.

6. Modify the IPVPN parameters as per the guidelines in [“Add IP VPN Configuration to Provider Hubs” on page 182](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

7. Click **OK**.

An Edit job is triggered and you are returned to the IPVPN page.

A confirmation message appears (with the job link) at the top of the page indicating that the job was created. You can click the job link to view the status of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page.

After the job completes successfully, the IP VPN configuration details are updated on the IPVPN tab.

RELATED DOCUMENTATION

[Manage a Site | 170](#)[About the Departments Page | 781](#)

Delete IP VPN Configuration from Provider Hubs

To delete an IP VPN configuration:

1. Click **Resources > Site Management**.

The Site Management page appears.

2. Click the provider hub *Site-Name* link to delete an associated IP VPN configuration.

The *Site-Name* page appears.

3. Select **IPVPN** tab.

4. Select the department VPN whose configuration you want to delete.

5. Click the **Delete** icon (trash can).

The Confirm Delete dialog box appears.

6. Click **Yes**.

A Delete IPVPN job is triggered and you are returned to the IPVPN page.

A confirmation message appears (with the job link) at the top of the page indicating that the job was created. You can click the job link to view the status of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page.

After the delete job completes successfully, the IP VPN configuration is removed from the IPVPN tab for the selected department VPN.

RELATED DOCUMENTATION

[Manage a Site | 170](#)

Viewing the Sites History

IN THIS SECTION

- [Viewing Jobs Initiated to Add and Configure Sites | 187](#)
- [Viewing Jobs Initiated to Delete Sites | 188](#)

Viewing Jobs Initiated to Add and Configure Sites

You can view the jobs initiated to add and configure all the sites in a tenant from the Sites page.

To view the jobs executed to add and configure sites:

1. Click **Resources > Site Management**.

The Sites page appears.

2. On the Sites page, click **More > View Add Site History**.

The Add/Configure Site History page appears. The Add/Configure Site History pane lists the jobs executed for adding and configuring all the sites in a tenant.

[Table 35 on page 187](#) describes the fields displayed on the Add/Configure Site History page.

Table 35: Fields on the Add/Configure Site History Page

Field	Description
In Progress	Number of jobs in progress.
Success	Number of jobs that were successfully executed.
Failure	Number of jobs that failed during execution.
Name	Name of the job executed to add a site. Click the hyperlinked name to open the Site History Tasks page, where the tasks executed to complete the job are listed. Click the task link to open the Job Status page, where you can view the date and time when various tasks were executed to complete the job.
Start Date	Date and time that the job was initiated.

Table 35: Fields on the Add/Configure Site History Page (*continued*)

Field	Description
End Date	Date and time that the job finished executing. If the job is in-progress or failed, no date is displayed.
Status	Indicates whether the job completed successfully (Success) or not (Failed).
Log	Link to the log generated for the job. Click the link to view the logs on the Job Status page. The Job Status page displays the date and time when the job and various tasks associated with the job were executed in chronological order.

Viewing Jobs Initiated to Delete Sites

To view jobs initiated to delete sites from a tenant:

1. Click **Resources > Site Management**.

The Sites page appears.

2. On the Sites page, click **More > View Delete History**.

The Delete History page appears. The Delete History page lists the all the jobs executed for deleting sites from a tenant.

[Table 36 on page 188](#) details the fields displayed on the Delete Site History page.

Table 36: Fields on the Site Delete History Page

Field	Description
In Progress	Number of jobs in progress.
Success	Number of jobs that were successfully executed.
Failure	Number of jobs that failed during execution.
Name	Name of the job executed to delete a site. Click the hyperlinked name to open the Site History Tasks page, where the tasks executed to complete the job are listed. Click the task link to open the Job Status page, where you can view the date and time when various tasks were executed to complete the job.

Table 36: Fields on the Site Delete History Page *(continued)*

Field	Description
Start Date	Date and time that the job was initiated.
End Date	Date and time that the job finished executing. If the job is in-progress or failed, no date is displayed.
Status	Indicates whether the job completed successfully (Success) or not (Failed).
Log	Link to the log generated for the job. Click the link to view the logs on the Job Status page. The Job Status page displays the date and time when the job and various tasks associated with the job were executed in chronological order.

SEE ALSO

[About the Site Management Page | 68](#)

[Delete a Site—Enterprise Hub, Cloud Spoke, and Branch | 213](#)

Edit Site Overview

IN THIS SECTION

- [Benefits of Editing Site Parameters | 192](#)

Tenant Administrator users can edit the parameters configured for a branch site or an enterprise hub site with the following site status:

- Configuration-Failed
- Partially-Provisioned
- Provisioned

- Managed
- Provision-Failed

NOTE:

- To edit a provisioned or a partially-provisioned provider hub site, the Operational Status of the site must be UP.
- Tenant Administrators can only edit the parameters of provider hub sites that they added.

You can add or delete WAN links, or modify the site parameters without affecting the connectivity to Contrail Service Orchestration (CSO).

For more information about how you can edit branch sites and enterprise hub sites parameters, see [“Edit Branch and Enterprise Hub Site Parameters” on page 192.](#)

NOTE: You cannot edit cloud spoke sites.

You can modify:

- Site properties: Address and Contact Information, Timezone, and so on.
- Network topology by:
 - Adding or deleting a WAN link
 - Modifying the properties of existing WAN links
 - Modifying the dynamic VPN (DVPN) thresholds of a site
 - Adding or deleting mesh tags on spoke sites or enterprise hub sites

What happens after you add a WAN link?

When you add WAN links to a branch site or enterprise hub site:

- Secure Operations, Administration, and Maintenance (OAM) tunnels are added between the spoke and hub sites if the **Use for OAM Traffic** option is enabled.
- Data links to provider hubs are established based on the overlay tunnel parameters configured for the WAN links.
- Data links to enterprise hubs are established based on the mesh tags configured on the spoke and enterprise hub sites.
- Monitoring of the new WAN link is enabled.

What happens to the existing DVPN and static tunnels when you modify the site parameters?

When you modify the DVPN thresholds configured for a WAN link, the changes you made do not reflect immediately. After the threshold for deleting tunnels is reached, the existing DVPN tunnels are deleted and new DVPN tunnels are added based on the modified DVPN parameters. If you want to see the changes you made immediately, manually delete the DVPN tunnels and add them again. For more information, see [“Adding On-Demand Mesh Tunnels” on page 244](#) and [“Deleting On-Demand Mesh Tunnels” on page 246](#).

When you modify the mesh tags for a WAN link, the changes you made do not automatically reflect in the static tunnels (existing between the spoke and an enterprise hub site, or between two enterprise hub sites) as this can cause data connectivity loss. To delete the existing static tunnels and add static new tunnels based on your modified parameters, you must reconfigure the static tunnels to apply the changes to the existing WAN link. To reconfigure the static tunnels, select **Reconfigure (Resources > Site Management > Site Name > WAN tab)** in Customer Portal. For more information, see [“Reconfigure Static Tunnels” on page 203](#).

What happens after you delete a WAN link?

When you delete a WAN link from a site, all the associated tunnels (secure OAM, data links to hub sites, and DVPN tunnels) are also deleted.

NOTE: Before deleting WAN links on:

- Spoke devices, ensure that at least one OAM WAN link is present is enabled for the site.
- NFX 250 dual CPE devices, ensure that atleast one OAM WAN link is present on both the CPE devices.
- Enterprise hubs, ensure that there are no static tunnels connected between the spoke sites and the enterprise hub using the WAN link.

What should you do if adding or deleting a WAN link fails?

If the addition or deletion of a WAN link fails, PARTIALLY DEPLOYED is displayed next to the WAN link name.

You can do one of the following:

- Retry the specific edit site job to execute the failed tasks from the Jobs page (**Monitor > Jobs**). For more information, see [“Retrying a Failed Job on Devices” on page 796](#).
- Redeploy the WAN link by clicking the **Re-Deploy WAN Link** toggle button and updating the WAN link parameters, which first deletes the WAN link and then adds it again.

NOTE: Redeploying a partially deployed WAN link can take several minutes based on the number of sites connected in a network.

- Leave the WAN link as is and redeploy the WAN link later.

Benefits of Editing Site Parameters

- Improves the user experience by enabling reconfiguration of the site by simply editing the site parameters without having to delete and add the site back.
- Simplifies the onboarding of a site. Initially, you can onboard a site by enabling only one OAM WAN link. You can later modify the site parameters to configure the site as per your business needs.

RELATED DOCUMENTATION

[About the Site Management Page](#) | 68

Edit Branch and Enterprise Hub Site Parameters

Tenant administrator users can modify the parameters configured for a branch site or an enterprise hub site from the Site Management page (**Resources > Site Management**).

NOTE: You cannot edit cloud branch sites.

To edit the parameters configured for a branch site or an enterprise hub site:

1. Select **Resources > Site Management**.

The Site Management page appears.

2. Select the site whose parameters you want to modify and click the **Edit** icon (pencil).

The Edit Site page appears, displaying the same fields that are presented when you add a site.

NOTE: You can edit the parameters of a site in any one of the following states:

- Configuration-Failed
- Partially-Provisioned
- Provisioned
- Provision-failed
- Managed

3. Modify the site parameters as described in:

- [Table 37 on page 194](#) for branch and enterprise hub sites.
- [Table 38 on page 202](#) for branch sites with Security Services (also referred to as next-generation firewall or NGFW) capability.

NOTE: You can upgrade a Secure SD-WAN Essentials site to a Secure SD-WAN Advanced site (allowed if the SD-WAN service level of the tenant is upgraded to Advanced) by selecting the Secure SD-WAN Advanced option from the site capability. You can also add secondary hubs to the upgraded sites, if required.

For more information on each parameter, see [“Add a Branch Site with SD-WAN Capability” on page 120](#) and [“Add Enterprise Hubs with SD-WAN Capability” on page 76](#).

4. (Optional) Review the configuration in the **Summary** tab and modify the parameters, if required.

5. Do one of the following:

- Click **Finish** to save the changes that you made to the provider hub site.
- Click **Previous** to make changes in the previous page.
- Click **Cancel** to discard the changes. A dialog box appears asking for your confirmation. Click **Yes**. The changes you made are lost and you are returned to the Site Management page.

If you click **Finish**, an Edit Site job is triggered and a job link appears on the Site Management page.

You can click the job link to view details of the job (including job status, start date and time, and end date and time). Alternatively, you can view the status of the job on the Jobs (**Monitor > Jobs**) page.

After the Edit Site job is completed successfully, a confirmation message indicating that the site is updated, appears on top of the Site Management page.

NOTE: The following operations take several minutes (greater than 15 minutes) based on the number of sites connected in the network:

- Deleting a WAN link
- Editing the following parameters of a WAN link:
 - Link Type
 - PPPoE
 - Address Assignment Method
 - Use for OAM Traffic
 - Backup Link
 - VLAN ID
- Redeploying a partially deployed WAN link

Table 37: Editable fields for a branch site and enterprise hub site

Editable Parameters	Site Type	Description
General		
NOTE:		
<ul style="list-style-type: none"> • To edit the WAN parameters of an on-premise spoke (branch) site or an enterprise hub site, ensure that the site version is 5.3.0 or higher. If the site version is of an earlier release, you must upgrade the site. For more information, see "Upgrading Sites" on page 211. • For on-premise spoke (branch) site or an enterprise hub site with 5.2.0 or earlier site versions, only advanced configuration fields are editable. You can find the version of a site in the Version column on the Site Management page. 		
Site Name	Enterprise hub site	Edit the name of the site.
	SD-WAN branch site	You can only use alphanumeric numbers and hyphen. The site name must be unique and the name length must not exceed 32 characters.

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
Device Host Name	Enterprise hub site	Edit the device host name for the site.
	SD-WAN branch site	<p>You can only use alphanumeric numbers and hyphen (-). The device host name must be unique and name length must not exceed 32 characters.</p> <p>Format: <tenant_name>.<site_name>.</p> <p>For example, TenantA.Orange.</p> <p>NOTE: The tenant name is always added as a prefix for the device host name. The tenant name part in the device host name cannot be edited.</p>
Address and Contact Information	Enterprise hub site	Edit the Street Address, City, State/Province, ZIP/Postal Code, Country, Contact Name, Email, or Phone Number.
	SD-WAN branch site	
Advanced Configuration	Enterprise hub site	Edit the Domain Name Server (DNS) IP address (IPv4 or IPv6, or both), Network Address Translation (NTP) Server IP address, or the selected Timezone.
	SD-WAN branch site	

Device

You can do one of the following:

- Edit enterprise hub and provider hub configuration.
- Edit the WAN parameters (specified below) of an existing WAN link.
- Add a new WAN link by clicking the toggle button next to the WAN link name and specifying the WAN parameters.
- Delete an existing WAN link by clicking the enabled toggle button next to the WAN link name.

NOTE: You cannot edit the device series (for example, NFX Series to SRX Series devices) as this change requires the site to be deleted and added again.

Hub Configuration

NOTE:

- You can edit the primary or secondary provider hub only if it is DATA_ONLY provider hub.
- You can also select **None** from the following hub configuration settings to run the SD-WAN site in a hub-less mode.

Primary Provider Hub	Enterprise hub site	Edit the primary provider hub device configured for the site.
	SD-WAN branch site	

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
Secondary Provider Hub	Enterprise hub site	Edit the secondary provider hub device configured for the site.
	SD-WAN branch site	NOTE: Not applicable to sites with SD-WAN Essentials service.
Primary Enterprise Hub	SD-WAN branch site	Edit the primary enterprise hub device configured for the site.
Secondary Enterprise Hub	SD-WAN branch site	Edit the secondary enterprise hub device configured for the site. NOTE: Not applicable to sites with SD-WAN Essentials service.
Use Mesh Tags to connect EHub	SD-WAN branch site	<p>This toggle button is enabled by default. If this button is enabled, CSO uses mesh tags to automatically form the overlay tunnel between the site and the enterprise hubs.</p> <p>Disable this toggle button if you want to manually create static tunnel (per WAN link) between the branch site and the enterprise hubs. If you disable this option, you must manually enable at least one WAN link to connect to the enterprise hub by using the Connects to Enterprise Hubs toggle button in the Advanced Settings of the WAN link.</p>

WAN Links

For each WAN link, you can edit the following properties:

Re-Deploy WAN Link	Enterprise hub site SD-WAN branch site	Click the toggle button to enable editing the WAN parameters of the partially deployed WAN link.
Link Type	Enterprise hub site SD-WAN branch site	Select MPLS or an Internet link.
Access Type	SD-WAN branch site	You cannot edit the Access Type field because you cannot add the same WAN link with different access types as it depends on the slots configured on the device. If needed, you can delete the WAN link and add a new WAN link.

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
PPPoE/PPP	SD-WAN branch site	<p>Click the toggle button to enable or disable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet) or PPP (Point-to-Point Protocol). You can enable PPPoE or PPP per WAN link. If you've enabled this toggle button for a WAN link, in the PPPoE/PPP Settings section, you can modify the username, password, and the authentication protocol. You can enable PPPoE or PPP on MPLS-based or internet-based WAN links.</p> <p>PPPoE works with Ethernet, ADSL, and VDSL access types while PPP works with the LTE access type.</p> <p>NOTE: The PPPoE/PPP toggle button is not supported for Internet links with LTE access type.</p>
Access Point Name (APN)	SD-WAN branch site	<p>Edit the access point name (APN), for the CPE device, which is specified by the service provider.</p> <p>This field is displayed only if you've enabled the PPPoE/PPP toggle button for MPLS links with LTE as the access type. If you've disabled the PPPoE/PPP toggle button for these links, CSO uses the default APN settings.</p>
Egress Bandwidth	Enterprise hub site SD-WAN branch site	Edit the maximum bandwidth (in Mbps) allowed for the WAN link.

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
Underlay Address Families	Enterprise hub site SD-WAN branch site	<ul style="list-style-type: none"> For enterprise hub sites—You can modify the Static IP Prefix and Gateway IP address of the device. For SD-WAN branch sites—Click either IPv4 or IPv6, or both IPv4 and IPv6 toggle buttons to enable either IPv4 or IPv6, or both IPv4 and IPv6 address assignment respectively, for the WAN link. If you enable IPv4 address assignment, you can modify the address assignment method to choose either STATIC or DHCP (Dynamic Host Configuration Protocol). If you enable IPv6 address assignment, you can choose STATIC, DHCP (router advertisement only), or SLAAC (Stateless Address Auto Configuration). If you select STATIC as the address assignment method, you can also modify the Static IP Prefix and Gateway IP address of the device. NOTE: For SD-WAN branch sites using Internet or MPLS links with LTE access type, you can select only the DHCP method for address assignment.
Public IP Address (Only for enterprise hub sites)	Enterprise hub site	Edit the public IPv4 address configured for the WAN link.
Advanced Settings		
Address Family (Tunnel Creation)	Enterprise hub site SD-WAN branch site	<ul style="list-style-type: none"> For enterprise hub sites—You can select only IPv4 as the underlay address family that is used to establish the overlay tunnel because enterprise hubs support only IPv4 address assignment. For SD-WAN branch sites—Select the underlay address family (IPv4 or IPv6) that is used to establish the overlay tunnel. The options on the list are populated based on the address family that you've configured for the underlay (either IPv4 or IPv6, or both).
Provider	Enterprise hub site SD-WAN branch site	Edit the Internet Service Provider (ISP) name.
Cost/Month	Enterprise hub site SD-WAN branch site	Edit the cost of using the WAN link per month (range is 1 through 10000). You can select the currency of the cost from the adjacent list.

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
Enable Local Breakout	Enterprise hub site SD-WAN branch site	<p>Click the toggle button to enable or disable the local breakout on the site.</p> <p>If you enabled local breakout, you can:</p> <ul style="list-style-type: none"> • Edit the Breakout Options to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic. • Click the Autocreate Source NAT Rule toggle button to enable or disable the automatic creation of source Network address translation (NAT) rules. If enabled, from the Translation list, you can edit the type of NAT to be used for the traffic (interface or pool). For pool-based NAT, you can edit one or more IP Addresses. <p>NOTE: Sites with Secure SD-WAN Essentials service support interface-based source NAT rules only. Sites with Secure SD-WAN Advanced service support both Interface-based or Pool-based source NAT rules.</p> <ul style="list-style-type: none"> • Click the BGP Underlay Options toggle button to enable or disable the BGP underlay routing. If enabled, you can edit Secondary Neighbor IP address, eBGP Peer-AS-Number, Local AS Number, Authentication for BGP route (none or MD5), whether you want to Advertise Public LAN Prefixes. <p>NOTE: Not applicable to sites with SD-WAN Essentials service.</p>
MAP-E	SD-WAN branch site	<p>Click the toggle button to enable or disable the Mapping of Address and Port with Encapsulation (MAP-E) functionality on the WAN link.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • MAP-E is compliant only with the Japan Network Enabler (JPNE) standards. • CSO supports MAP-E only on NFX150 devices with IPV6 address assignment and local breakout enabled for the WAN link.

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
Use For Fullmesh	Enterprise hub site SD-WAN branch site	<p>Click the toggle button to specify whether the WAN link can be a part of a full mesh topology. If enabled, you can edit:</p> <ul style="list-style-type: none"> Mesh overlay link type: If the link type is MPLS, select GRE-IPSEC or GRE as the mesh overlay link. If the link type is Internet, the value for mesh overlay link type is GRE_IPSEC. <p>NOTE: If you've enabled IPv6 address assignment for the WAN links, you can select only GRE-IPSEC as the type of mesh overlay link.</p> <ul style="list-style-type: none"> Mesh tags: Select the associated mesh tags for on-demand tunnel creation. <p>NOTE: For branch sites, you can select only one mesh tag for each WAN link. For enterprise hubs, you can select one or more mesh tags for each WAN link.</p>
Use for OAM Traffic	Enterprise hub site SD-WAN branch site	Click the toggle button to enable or disable sending the OAM traffic over the WAN link.
Connects to Enterprise Hubs		<p>This field is displayed only if you have enabled the Use Mesh Tags to Connect EHub field in the Hub Configuration section.</p> <p>Enable this toggle button if you want to manually connect the site to an enterprise hub, without using mesh tags.</p>
Primary EHub Tunnel Type		<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the tunnel type to be used for the connection between the branch site and the primary enterprise hub.</p>
Primary EHub Peer Device		<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Displays the name of the primary enterprise hub you have selected.</p>
Primary Ehub Peer Interface		<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the primary enterprise hub WAN link that needs to be part of the tunnel. You can select multiple WAN links.</p>

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
Secondary EHub Tunnel Type		<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the tunnel type to be used for the connection between the branch site and the secondary enterprise hub.</p>
Secondary EHub Peer Device		<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Displays the name of the secondary enterprise hub you have selected.</p>
Secondary Ehub Peer Interface		<p>This field is displayed only if you have enabled the Connects to Enterprise Hubs field.</p> <p>Select the secondary enterprise hub WAN link that needs to be part of the tunnel. You can select multiple WAN links.</p>
Connects to Hubs	Enterprise hub site SD-WAN branch site	<p>NOTE: The Connects to Hubs field is available only if you have selected a provider hub.</p> <p>Click the toggle button to specify whether or not the WAN link of the site connects to a hub. If enabled, you can edit:</p> <ul style="list-style-type: none"> • Overlay Tunnel Type: If the link type is MPLS, select GRE-IPSEC or GRE as the overlay tunnel type. If the link type is Internet, the value for tunnel overlay link type is GRE_IPSEC. • Overlay Peer Interface: Modify the interface name of the hub device to which the WAN link of the site is connected.
Backup Link	Enterprise hub site SD-WAN branch site	Click the toggle button to enable or disable the backup link through which traffic can be routed when the primary link is unavailable.
Default Link	Enterprise hub site SD-WAN branch site	Click the toggle button to enable or disable the default link through which traffic can be routed when matching SD-WAN policy intents are unavailable.
Data VLAN ID	Enterprise hub site SD-WAN branch site	<p>Edit the VLAN ID.</p> <p>Range: 0 through 4049 (4050 to 4094 is reserved by CSO).</p>

Table 37: Editable fields for a branch site and enterprise hub site (*continued*)

Editable Parameters	Site Type	Description
---------------------	-----------	-------------

Advanced Configurations

NOTE: Sites with SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or a tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.

DVPN Threshold for Tunnel Creation	Enterprise hub site SD-WAN branch site	Edit the number of sessions specified for the Threshold for Tunnel Creation.
DVPN Threshold for Tunnel Deletion	Enterprise hub site SD-WAN branch site	Edit the number of sessions specified for the Threshold for Tunnel Deletion.

Table 38: Editable fields for branch sites with NGFW capability

General

Address and Contact Information	Edit the Street Address, City, State/Province, ZIP/Postal Code, Country, Contact Name, Email, or Phone Number.
Advanced Configuration	Edit the Domain Name Server (DNS) IP address, Network Address Translation (NTP) Server IP address, or the selected Timezone.

Device Information

Secure Log Source Interface	Edit the port configured as the management interface to connect to a management device. You can configure any of the ge-0/0/x ports (x ranging from 0 to 14) as in-band management interfaces.
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

RELATED DOCUMENTATION

[Manually Adding Branch Sites | 119](#)

[Add a Branch Site with SD-WAN Capability | 120](#)

Reconfigure Static Tunnels

Contrail Service Orchestration (CSO) creates static overlay tunnels between a branch site and an enterprise hub site or between two enterprise hub sites, based on matching mesh tags associated with the WAN link.

If you modify the mesh tags for a WAN link while editing a branch or an enterprise hub site, the existing static tunnels are not updated. To apply the changes that you made to the WAN link, you must manually reconfigure the static tunnels.

NOTE:

- To reconfigure the static tunnels associated with a provider hub site, you must edit the site and update the overlay tunnel information in the **Connects to Hubs** (Overlay Tunnel Type and Overlay Peer Interface) fields.
- We recommend that you reconfigure the static tunnels during a downtime or when traffic between the sites is not expected because reconfiguring the existing static tunnels can result in connectivity loss between the sites in the tenant.

A Tenant Administrator user can reconfigure static tunnels between a branch site and an enterprise hub site or between two enterprise hub sites in the Customer Portal.

To reconfigure static tunnels for a site:

1. Click **Resources > Site Management**.

The Site Management page appears.

2. Click the *Site-Name* link of the site for which you want to reconfigure the static tunnels.

The *Site-Name* page appears.

3. On the **WAN** tab, click **Reconfigure**.

The Reconfigure Static Tunnel page appears.

4. In the **Destination Name** list, enter or select the names of one or more destination sites for which you want to reconfigure the static tunnels.

5. Click **OK** to save the changes.

A Reconfigure Static Tunnel job is triggered and you are returned to the *Site-Name* page. You can click the job link to view details of the job (including job status, start date and time, and end date and time). Alternatively, you can view the status of the job on the Jobs (**Monitor > Jobs**) page.

After the job completes successfully, the static tunnels are reconfigured between the source and the destination sites that you selected. On the **WAN** tab of *Site-Name* page, the overlay topology graphic is updated with the reconfigured static tunnels.

If the Reconfigure Static Tunnel job fails, you can retry the failed job from the Jobs page or attempt to reconfigure the static links again.

RELATED DOCUMENTATION

[Edit Branch and Enterprise Hub Site Parameters | 192](#)

[Retrying a Failed Job on Devices | 796](#)

Edit Site Examples

This topic provides examples on how you can use the edit site feature to configure a site for different real-time deployment scenarios. Once you have onboarded a site, you can easily configure a site by modifying the required site parameters without disrupting traffic through the site.

We start with an SD-WAN site connected to CSO through an OAM WAN link. You require only one OAM WAN link to onboard a site using ZTP.

Figure 5: A Simple SD-WAN Site

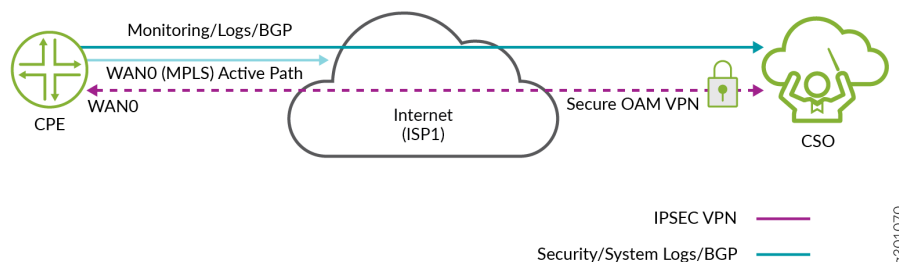


Figure 5 on page 204 shows a simple site onboarding topology with a single WAN link (WAN0). The WAN0 link has secure OAM tunnels and iBGP peering with vRR configured on it. Stage-2 configurations can be applied to the device.

You can now edit the site properties to deploy services such as SD-WAN or NGFW on this site.

Figure 6 on page 205 shows a remote site with a LAN segment, and an active WAN link (WAN0) with local breakout and automatic NAT rule creation enabled. For information on adding LAN segments, see “[Managing LAN Segments on a Tenant Site](#)” on page 161.

Traffic passes through the WAN0 link to the internet or cloud applications.

To enable local breakout and autcreate NAT rules on the WAN0 link, on the **WAN** tab of the Edit Site page, in the **Advanced Settings**, click **Enable Local Breakout** and **Autcreate Source NAT Rule** toggle buttons. Post activation of the site, basic firewall policy is auto-deployed on the WAN0 link.

Example 2: Configure a Site with a LAN Segment, Active WAN Link, Backup WAN Link, and Local Breakout Enabled

Figure 7: A CPE Site with a LAN Segment, Active WAN link, and Backup WAN Link

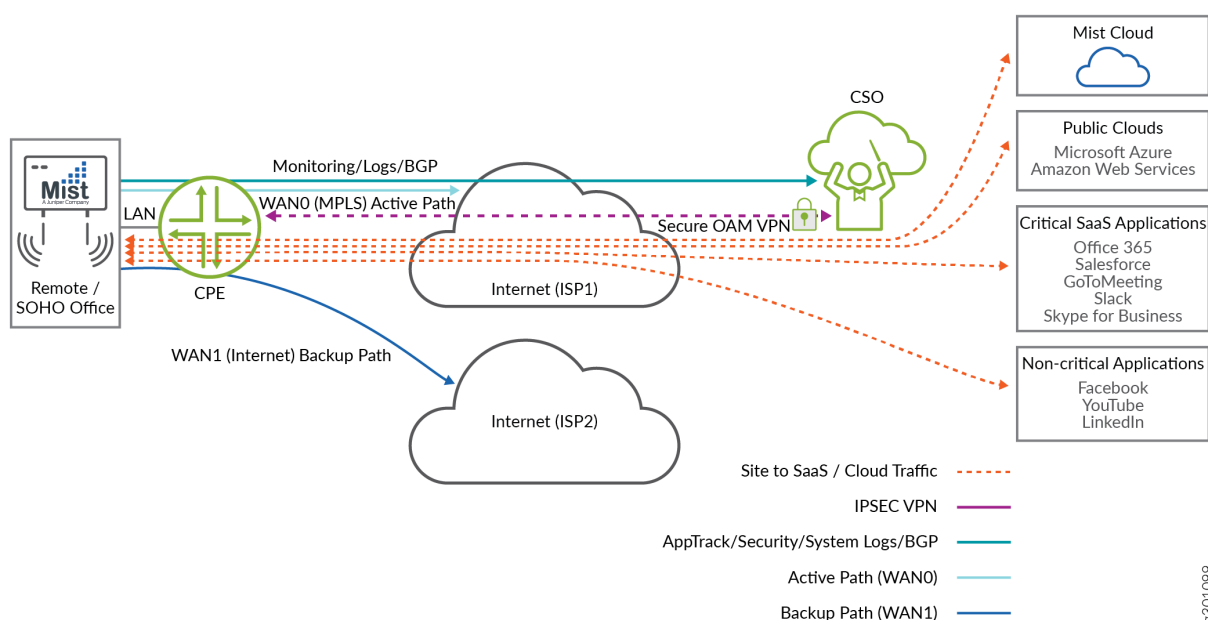


Figure 7 on page 206 shows an alternative deployment scenario to “[Example 1: Configure a Site with a LAN segment, WAN link, and Local Breakout Enabled](#)” on page 205 by adding a backup WAN link (WAN 1).

To add the WAN1 backup link, on the **WAN** tab of the Edit Site page:

1. Enable an additional WAN link by clicking the toggle button on the right of the WAN link.
2. In the **Advanced Settings** of the newly enabled WAN link, click the **Backup Link** toggle button.

The site now has local breakout with automatic NAT rule creation enabled on both the WAN links (WAN0 and WAN1). By default, the traffic goes through the WAN0 link. If there is a failure on WAN0 link, the traffic is directed to the WAN1 link.

Example 3: Configure a Site with a LAN Segment and Two Active WAN Links

Figure 8: A CPE Site with a LAN Segment and Two Active WAN Links

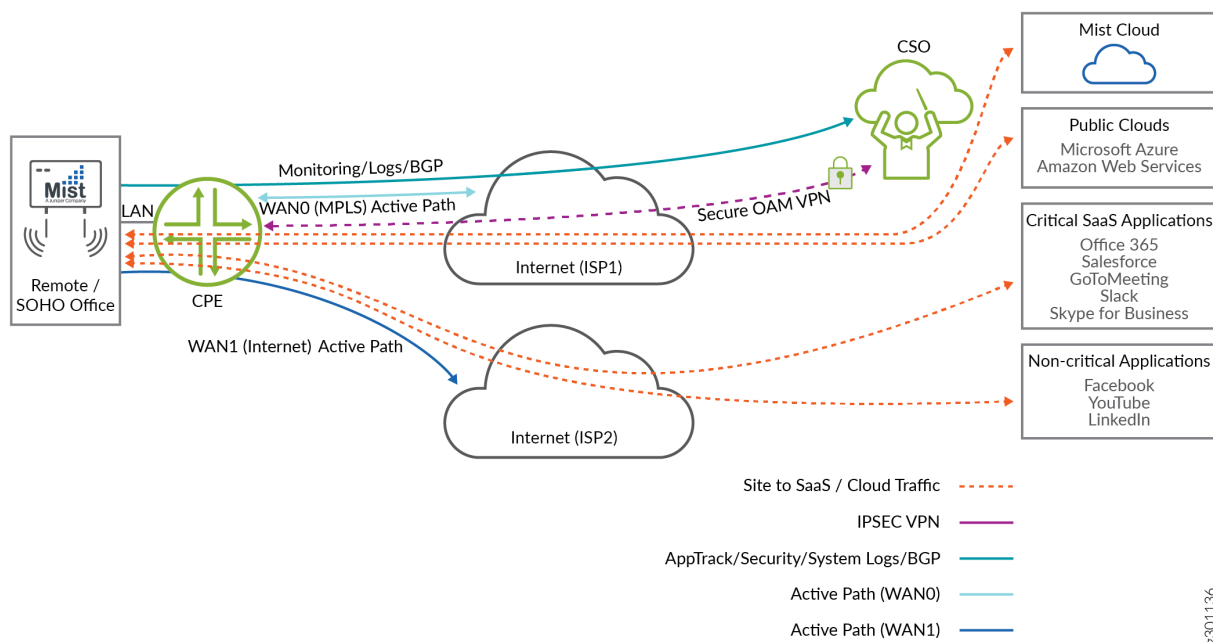


Figure 8 on page 207 shows an alternative deployment scenario to [Example 2: Configure a Site with a LAN Segment, Active WAN Link, Backup WAN Link, and Local Breakout Enabled on page 206](#). You can configure the SDWAN policy such that some applications use MPLS link and others use Internet links. In this example, the site is configured with two active WAN links: WAN0 as an MPLS link and WAN1 as an Internet link.

To edit the link type of a WAN link, on the **WAN** tab of the Edit Site page, select **MPLS** or **Internet** from the **Link Type** list.

You can add two active WAN links or change the backup link to an active link.

To change the backup link to an active link, in the **Advanced Settings** of the selected WAN link, disable the **Backup Link** toggle button.

The application traffic passes through both the active links based on the type of traffic from different applications. In this example, for traffic from non-critical applications like YouTube, an Internet link is used.

Example 4: Configure a Site integrated with Zscaler

Figure 9: A CPE with a LAN Segment, Two Active WAN Links, and Integrated with Zscaler

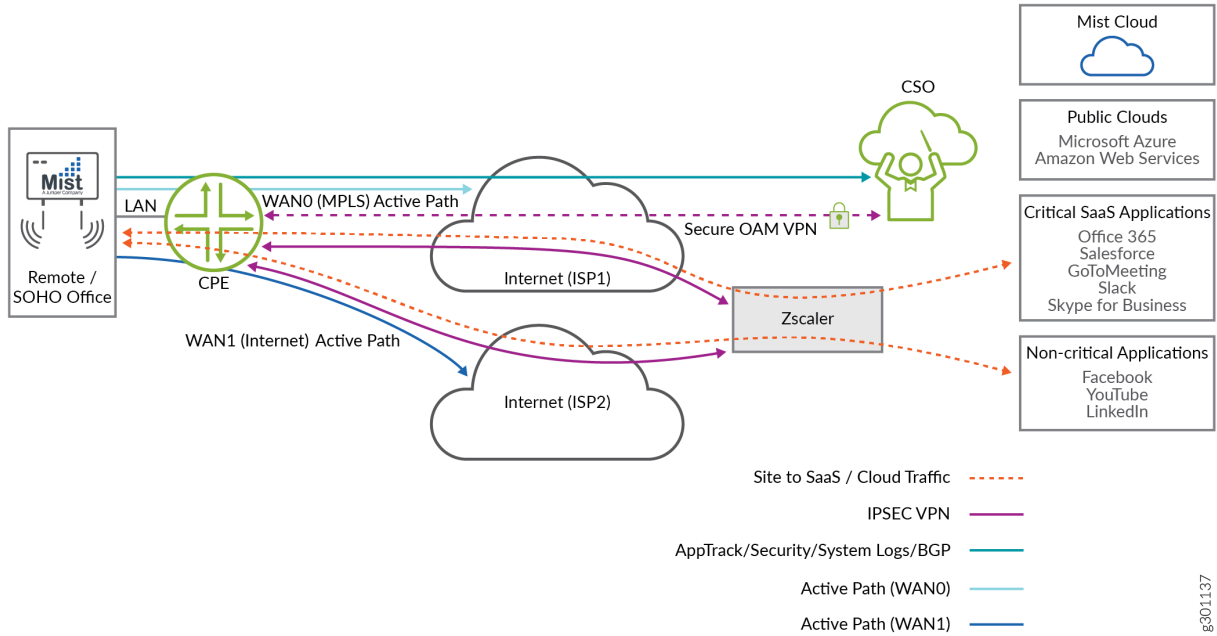


Figure 9 on page 208 shows Zscaler, a cloud-based security platform, integrated to the active WAN1 link. If you select the cloud breakout option, GRE or IPsec tunnels are formed between the CPE device to the Zscaler device and all internet traffic breaks through this tunnel. For more information, see [“Adding Cloud Breakout Settings”](#) on page 616.

Example 5: Configure Site-to-Site Traffic Through DVPN Tunnels

Figure 10: Two CPEs Connected Through DVPN Tunnels Without Hub

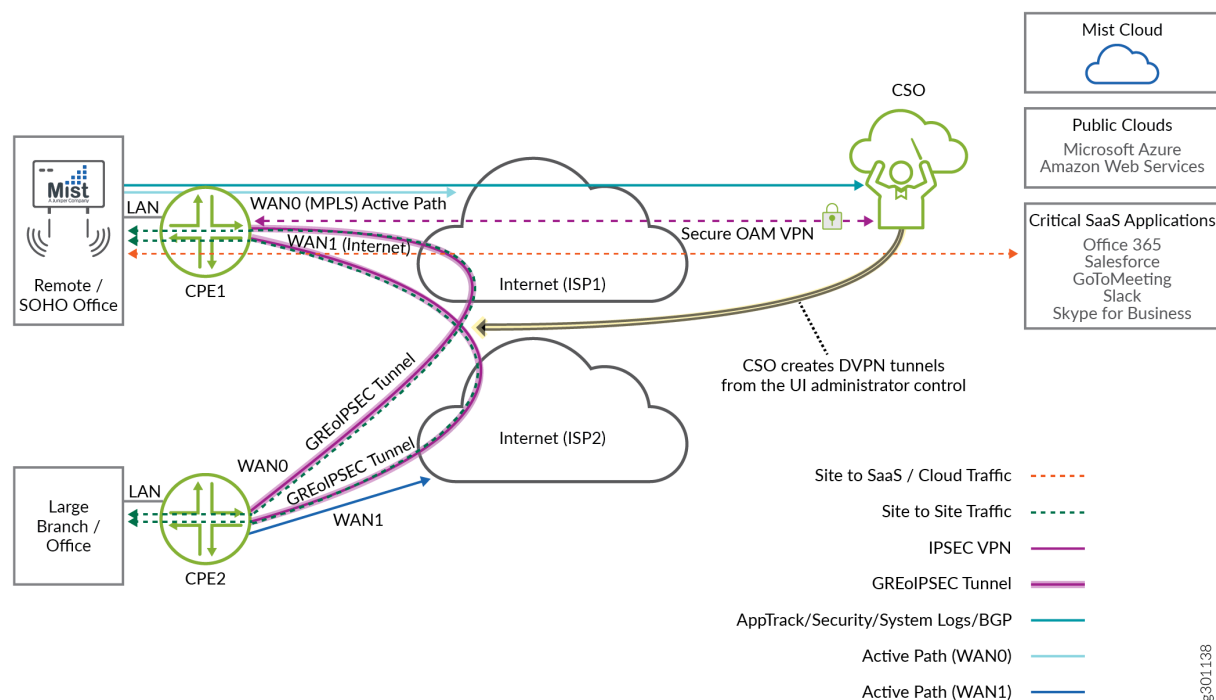


Figure 10 on page 209 shows a deployment scenario with two SD-WAN CPEs connected through Dynamic VPN (DVPN) tunnels, without connecting to any hubs.

To enable the DVPN tunnels between the two CPEs:

- Enable full mesh on the WAN links
- Add matching mesh tags on the WAN links

To enable full mesh a WAN link and select the required mesh tag, on the **WAN** tab of the Edit Site page, in the **Advanced Settings**:

1. Click **Use For Fullmesh** toggle button
2. Select the required **Mesh tag** from the list.

Upgrading Sites

IN THIS SECTION

- [Upgrading Junos OS | 211](#)
- [Upgrading a Site | 212](#)
- [Upgrading Sites in Bulk | 213](#)

You can upgrade one or more sites from the Customer Portal > Site Management page.

Upgrading Junos OS

Before you upgrade a site, you must upgrade the Junos OS on the device. The minimum required Junos OS release is 20.4R2. To upgrade the image:

1. In the Customer Portal, select **Resources > Images**.

The Images page appears.

2. Select the device image to be staged on the device and click the **Stage** button.

The Stage Image: Select Devices page appears.

3. Select the device onto which the device image needs to be staged.
4. Select **Run now** if you want to stage the image immediately. Select **Schedule at a later time** if you want to schedule the staging for a later date and time.
5. Click **OK**.

You are returned to the Images page. If you selected **Run Now** in Step 4, then you must wait for the confirmation message that staging is complete before proceeding with the next step.

6. Ensure that the staged image is selected and click the **Deploy** button .

The Deploy Image: Select Devices page appears.

7. Select the device onto which the device image needs to be deployed. Disable the **Stage Image** toggle button.
8. Select **Run now** if you want to deploy the image immediately. Select **Schedule at a later time** if you want to schedule the deploy for a later date and time.
9. Click **OK**.

Upgrading a Site

NOTE:

- When you request Request Material Authorization (RMA) on a site that is associated with a single-CPE device and has a version earlier than the current CSO version, the site version is upgraded to the CSO version. The site version is upgraded as part of the device activation and zero touch provisioning (ZTP) process of the replacement device that is performed after the RMA.
- On a site associated with an NFX dual-CPE device, if the site version is lower than that of the CSO version, you can perform RMA only at the cluster level. After RMA of the cluster, the version of the site is upgraded to that of CSO as part of the device activation and ZTP process of the replacement devices in the cluster.

To upgrade a site:

1. In Customer Portal, select **Resources > Site Management**.

The Site Management page appears.

2. View the list of sites, and based on the Site Status column identify whether the site requires an upgrade.

If the Site Status is **Provisioned**, the upgrade is optional. If the site status is **UPGRADE-REQUIRED**, the site upgrade is mandatory.

You cannot upgrade a site if the site status is **Created**, **Provision Failed**, **Configured**, and **Activation Failed**.

3. Select a site and click **More > Upgrade**. The Upgrade Site:SiteName page appears.

4. Click **OK**.

CSO triggers an upgrade job and displays a confirmation message with a job ID link. You are returned to the Site Management page. You can click the link in the message to view the details of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page.

When a site is upgraded successfully, the version number of the site matches the CSO version and the management status is set to **Provisioned**.

Upgrading Sites in Bulk

To upgrade sites in bulk:

1. In the Customer Portal, select **Resources > Site Management**.

The Site Management page appears.

2. View the list of sites, and based on the Site Status column identify whether the site requires an upgrade.

If the site status is provisioned, the upgrade is optional. If the site status is UPGRADE-REQUIRED, the site upgrade is mandatory.

You cannot upgrade a site if the site status is Created, Provision Failed, Configured, and Activation Failed.

3. Select one or more sites, and click **More > Upgrade**.

The Upgrade Site page appears.

4. Click **Upgrade**.

A job is created. Click the job ID to go to the Jobs page and view the status of the upgrade. All sites meeting the required criteria are upgraded. When a site is upgraded successfully, the version number of the site matches the CSO version and the management status is set to **Provisioned**.

RELATED DOCUMENTATION

| [Upgrading Sites Overview](#) | 75

Delete a Site—Enterprise Hub, Cloud Spoke, and Branch

You can delete a site from the Sites page (**Resources > Site Management**) in Customer Portal.

The following are applicable when you want to delete a site:

- You can delete only one site at a time.
- You cannot delete an enterprise hub or a provider hub site that are associated with a spoke site. You must first delete the spoke sites associated with the enterprise hub or provider hub site and then delete the enterprise hub or provider hub site.

- You cannot delete a site that is associated with site-specific policies. You must first delete the intents in the policy that are associated with the site, redeploy the policy, and then delete the site.
- You cannot delete a site that has service instances associated with it. So, before attempting to delete a site, delete service instances associated with the site. See *Delete a Network Service*.

To delete a site:

1. Click **Resources > Site Management**.

The Sites page appears.

2. Select the site that you want to delete and click the delete (trash can) icon.

The Remove Site Options dialog box appears.

3. Select one of the following options:

- **Load Recovery Configuration**—Use this option to back up any custom configuration on the device that is present on the device when you trigger site deletion. CSO restores the custom configuration when you reinstall the device.
- **Zeorize the device**—Use this option to reset the device to the factory default configuration.

NOTE: When you zeroize the device, you will lose custom configurations on the device.

4. Click **OK**.

CSO triggers a job to delete the site is created. After the job completes successfully, a message appears on top of the Sites page indicating that the site is deleted.

Starting in CSO Release 6.1.0, the site deletion process is split into two phases to minimize the overall time required to delete a site:

- **Site deletion (phase 1)**—The device is zeroized, all activation information is removed from CSO, and the site is deleted from the GUI. After deletion, you can onboard the site using the same name or a different name.
- **Site cleanup (phase 2)**—The cleanup process is triggered after the site is deleted. This process removes all the configuration associated with the site from the provider or enterprise hub, a spoke site to which this site is connected, and virtual Route Reflectors (vRRs).

NOTE: For optimization purposes, configurations on spoke sites might not be deleted during the cleanup phase. In such cases, the configurations are deleted during the next commit operation on the spoke devices.

If the delete site (phase 1) operation is unsuccessful, you cannot add a new site that uses the same site name as the site that you attempted to delete. However, if the site cleanup (phase 2) is unsuccessful, you can add a new site with the same name as the deleted site.

RELATED DOCUMENTATION

[About the Site Management Page | 68](#)

[Contrail Service Orchestration Monitoring and Troubleshooting Guide](#)

Managing Site Groups

IN THIS CHAPTER

- [About the Site Groups Page | 216](#)
- [Creating Site Groups | 217](#)

About the Site Groups Page

To access this page, click **Resources > Site Groups**.

You can use the **Site Groups** page to view, create, and delete site groups for a tenant. Site groups enable you to group sites logically, thereby easing site management. You can use site groups to apply policies at the site group level.

You must be a Tenant Administrator user to access the **Site Groups** page.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of existing site groups. Click the details icon that appears when you hover over the name of a site group or select **More > Detailed View**.
- Create site groups. See [“Creating Site Groups” on page 217](#).
- Edit site groups. Select a site group and click the edit icon. If you add a site to (or remove a site from) a site group that is selected in a firewall policy, you need to manually redeploy that policy.
- Delete site groups. To delete a site group, select it on the Site Groups page and click the delete (X) icon.

NOTE: You cannot delete a site group selected in a firewall policy.

Field Descriptions

Table 39 on page 217 shows the descriptions of the fields on the **Site Groups** page.

Table 39: Fields on the Site Groups Page

Field	Description
Name	Displays the name of the site group.
Sites	Displays the names of the sites that are members of a site group.

RELATED DOCUMENTATION

| [Creating Site Groups](#) | 217

Creating Site Groups

You can use the **Create Site Group** page to create a new site group for a tenant and add sites to it.

To create a site group:

1. Click **Resources > Site Groups**.
The Site Groups page appears.
2. Click the add icon (+).
The **Create Site Group** page appears.
3. Enter a unique name for the site group.
4. From the list of sites in the **Available** column, select the sites that you want to include in the new group and click the greater-than icon (>).
The selected sites are moved to the **Selected** column.
5. Click **OK**. If you want to discard your changes, click **Cancel** instead.
The new site group is displayed on the **Site Groups** page.

RELATED DOCUMENTATION

| [About the Site Groups Page](#) | 216

Managing Site Templates

IN THIS CHAPTER

- [About the Site Templates Page | 219](#)
- [Add Branch Sites by Using a Site Template | 220](#)
- [Cloning, Editing, and Deleting Site Templates | 221](#)
- [Adding a Site Template | 224](#)
- [Adding and Configuring Sites by Importing a JSON File | 238](#)

About the Site Templates Page

To access this page, click **Resources > Templates > Site Templates**.

You can use the Site Templates page to add site templates, edit, clone, delete, and view existing site templates.

A site template enables you to specify values for many of the attributes used to add a site. You can then use the site template to add multiple sites that share the same set of values (for attributes already specified in the site template) and only specify values for site-specific attributes.

Site templates are available only for branch sites.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a site template. See [“Adding a Site Template” on page 224](#)
- Edit, clone, or delete site templates. See [“Cloning, Editing, and Deleting Site Templates” on page 221](#).
- View site template details. The site templates are displayed in card format. For each site template you can view the following details:
 - Template name
 - Published by
 - Capability type

- Number of devices attached
- Number of WAN links, if applicable
- Number of sites that the device template is attached to
- Date and time that the template was last updated

Add Branch Sites by Using a Site Template

Using a site template, you can add branch sites in bulk either manually or by importing the JavaScript Object Notation (JSON) file that contains branch site attributes.

To add branch sites by using a site template:

1. Select **Resources > Site Management**.

The Sites page appears.

2. Click **Add** and select **Branch Site (Using Site Template)**.

The Add Branch Site page appears.

3. Click **Add Site Template**.

4. Select the site template and click **Continue**.

The Add Branch Site page appears.

5. The **Site Template** field displays the name of the site template that you have selected. If you want to change the site template, click the **Change** link and select another site template of your preference from the Add Branch Site page.

6. Do one of the following to add branch sites:

- To add branch sites in bulk by importing the JSON file:
 - a. Select **Import from JSON** in the Site Data field.
 - b. (Optional) Click **Download Sample JSON** to download a sample JSON template and use it to specify site data that you can later import.
 - c. Click **Browse** to upload the JSON file.
 - d. Navigate to the folder and select the JSON file.
 - e. Click **Open**.

- To manually add branch sites in bulk, select **Add Manually** in the Site Data field.

The Site 0 tab appears listing the fields based on the capabilities that were selected for the site template.

7. Complete the configuration for Site0.

For more information on the fields for adding a branch site with the following capabilities:

- WAN capability as SD-WAN, see [“Add a Branch Site with SD-WAN Capability” on page 120](#).
- WAN capability as Next Gen Firewall, see [“Add a Standalone Next-Generation Firewall Site” on page 153](#).

8. Click the plus icon (+) to add more sites and complete the configuration for each site.

9. Review the sites.

If there are validation errors, an error icon appears in the left pane (next to the site name). You must ensure that all errors are resolved before proceeding.

10. (Optional) You can remove a site by clicking the X icon when you hover over the site name in the left pane.

11. Click **Save**.

A confirmation message is displayed indicating that the job is created for adding sites in bulk.

RELATED DOCUMENTATION

[Adding a Site Template | 224](#)

[About the Site Templates Page | 219](#)

[Cloning, Editing, and Deleting Site Templates | 221](#)

Cloning, Editing, and Deleting Site Templates

IN THIS SECTION

- [Cloning Site Templates | 222](#)
- [Editing Site Templates | 222](#)
- [Deleting Site Templates | 223](#)

You can clone, edit, or delete a site template.

Cloning Site Templates

You can clone a site template when you want to quickly create a copy of an existing site template.

To clone a site template:

1. Select **Resources > Templates > Site Templates**.

The Site Template page appears.

2. Select the site template that you want to clone.

3. Click **Clone**.

The Clone Site Template page appears.

4. Specify a unique name for the site template that can contain alphanumeric characters and hyphens (-); the maximum length is 32 characters.

5. Click **OK** to save your changes.

A confirmation message appears, indicating the status of the clone operation.

The site template that you have cloned is displayed on the Site Templates page. You can modify the cloned site template as needed by clicking the edit icon.

Editing Site Templates



WARNING: You cannot edit a site template if you have associated the site template with a site.

To edit a site template:

1. Select **Resources > Templates > Site Templates**.

The Site Template page appears.

2. Select the site template that you want to edit.

3. Click the edit icon (pencil) to modify the parameters.

The Edit Site Template page appears.

4. Edit the fields, as needed. Modify the fields according to the guidelines provided in [“Adding a Site Template” on page 224](#).

NOTE: You cannot edit the site template name.

5. Click **OK** to save your changes.

A confirmation message appears, indicating the status of the edit operation. You can use the modified site template for creating multiple branch sites.

Deleting Site Templates



WARNING: You cannot delete a site template if you have associated the site template with a site.

To delete a site template:

1. Select **Resources > Templates > Site Templates**.

The Site Template page appears.

2. Click the site template that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the site template.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

[About the Site Templates Page | 219](#)

[Adding a Site Template | 224](#)

[Add Branch Sites by Using a Site Template | 220](#)

Adding a Site Template

You can add a site template for a branch site. A site template can be added with Security (also referred to as next-generation firewall or NGFW) or SD-WAN capabilities.

To add a site template:

1. Select **Resources > Templates > Site Templates**.

The Site Templates page appears.

2. Click the + icon.

The Add Site Template page appears.

3. Complete the configuration according to the guidelines in [Table 40 on page 224](#).

The last column of [Table 40 on page 224](#) indicates the capabilities for which a field is applicable.

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

The site template is added and listed in the Site Templates page. You can use the site template to add multiple branch sites.

Table 40: Fields on the Add Site Template Page

Field	Description	Applicable To
General Tab		
Template Name	Specify a unique name for the site template that can contain alphanumeric characters and hyphens (-); the maximum length is 32 characters.	
Template Description	Enter a description for the site template; the maximum length is 512 characters.	
Site Information		
Site Group	Select a site group to which you want to assign the template. Example: sdwan-spoke	

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Site Capabilities		
Site Capabilities	<p>Select one of the following capabilities for the site template:</p> <ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced <p>NOTE:</p> <ul style="list-style-type: none"> • The WAN capabilities that are displayed here are filtered based on the service type that are assigned to the tenant. 	
Configuration		
Primary Enterprise Hub	Select the primary enterprise hub with which you want to connect the branch site. If you specify a enterprise hub, then the initial site-to-site traffic as well as the central breakout (backhaul) traffic (if applicable) is sent through the enterprise hub instead of the hub site.	SD-WAN
Secondary Enterprise Hub	<p>Select the secondary enterprise hub for this branch site.</p> <p>The branch site connects with secondary enterprise hub when the primary enterprise hub is down.</p>	SD-WAN
Create Threshold	<p>Enter the maximum number of sessions closed between the connected sites in a duration of two minutes at which full mesh is created between the two sites.</p> <p>The default value is 5.</p> <p>For example, if you specify the number of sessions as 5, dynamic mesh tunnels are created if the number of sessions closed between two branch sites in 2 minutes exceeds 5.</p>	SD-WAN
Delete Threshold	<p>Enter the number of sessions closed between the connected sites in a duration of 15 minutes below which full mesh is deleted between the two sites.</p> <p>The default value is 2.</p> <p>For example, if you specify the number of sessions closed as 2, dynamic mesh tunnels are deleted if the number of sessions closed is lesser than or equal to 2.</p>	SD-WAN

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Address and Contact Information		
Street Address	Enter the street address of the site.	
City	Enter the city where the site is located.	
State/Province	Select the state or province where the site is located.	
ZIP/Postal Code	Enter the postal code for the site.	
Country	<p>Select the country where the site is located. Click the Validate button to verify the address. The site address verification successful message is displayed if the address is correct. You can click the View location on a map link to see the address location.</p> <p>If you enter the wrong address and click the Validate button to verify the address, the Site address could not be validated message is displayed .</p>	
Contact Name	Enter the name of the contact person at the site.	
Email	Enter the e-mail address of the contact person at the site.	
Phone	Enter the phone number for the site.	
Advanced Configuration		
Domain Name Server (DNS)	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on..</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>	
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>	
Select Timezone	Select the time zone in which the site is located from the drop-down list.	

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Device Tab		
Device Redundancy	Enable this option only for dual CPEs.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Device Series	<p>Select the device series to which the CPE belongs (SRX, NFX150, or NFX250) and select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Device Model	Select a device model from the list.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Zero Touch Provisioning	<p>Click the toggle button to enable or disable Zero Touch Provisioning (ZTP). This option is enabled by default.</p> <p>If ZTP is enabled, the Boot Image field is displayed and you must select an image that supports the Phone-Home client. During ZTP, the image on the firewall device is upgraded to the image that you select for the Boot Image.</p> <p>If ZTP is disabled, you must manually copy (by using CLI), the Stage-1 configuration on to the device.</p>	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Is Cluster Already Formed?	Click the toggle button to confirm whether the cluster is formed.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Cluster ID	Enter the device Cluster ID. The value is ignored if the cluster is already formed on the device. Cluster ID must be unique if more than one cluster is connected through the same switch.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the CPE when the CPE is detected by CSO (management status of the device is Device_Detected).</p> <p>When you enable this field, zero-touch provisioning of the device is automatically triggered after the site with the CPE is added to CSO.</p>	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Boot Image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the CPE device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image (NFX or SRX) is populated based on the device template that you have selected while adding a site. See <i>Uploading a Device Image</i>.</p>	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced

Management Connectivity

NOTE: This section is displayed only when Zero Touch Provisioning is disabled. If you enabled device redundancy, enter the information for both the nodes.

Table 40: Fields on the Add Site Template Page (continued)

Field	Description	Applicable To
Interface Name	Enter the management interface.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Access Type	Select the access type for the underlay link. LTE, ADSL, and VDSL access types are supported only on Internet links. You cannot add LTE, ADSL, and VDSL access types to the same WAN link.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Address assignment	By default, DHCP is selected. If you want to enter a static IP address, select STATIC.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
DATA VLAN ID	Enter a VLAN ID for the WAN link.	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced
PPPoE	Click the toggle button to enable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet).	<ul style="list-style-type: none"> • Device Management • Security Services • Secure SD-WAN Essentials • Secure SD-WAN Advanced

Table 40: Fields on the Add Site Template Page (continued)

Field	Description	Applicable To
Secure Log Source Interface	Select the port that you want to configure as management interface and connect it to the management device. You can configure any of the ge-0/0/x ports, where x ranges from 0 to 14, as in-band management interfaces.	Security Services
Firewall Policies	Select the firewall policy that you want to deploy. The firewall policy list is populated from the Configuration > Firewall > Firewall Policy page.	Security Services
NAT Policies	Select the NAT policy that you want to deploy to the standalone firewall site. The NAT policy list is populated from the Configuration > NAT > NAT Policies page.	Security Services (Next Gen Firewall)
Hub Configuration		
Primary Provider Hub	Select a primary data hub for the SD-WAN site.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Secondary Provider Hub	Select a secondary data hub for the SD-WAN site.	<ul style="list-style-type: none"> Secure SD-WAN Advanced
Primary Enterprise Hub	Select a primary gateway hub for the SD-WAN site.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Secondary Enterprise Hub	Select a secondary gateway hub for the SD-WAN site.	<ul style="list-style-type: none"> Secure SD-WAN Advanced
WAN 0	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN_0 link is enabled.</p> <p>When you enable a WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured.</p>	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Link Type	Select the underlay network type (MPLS or Internet) of the WAN link that is connected to the branch site.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Access Type	<p>Select the access type for the underlay link.</p> <ul style="list-style-type: none"> If you selected Internet as the link type, you can select Ethernet (default), LTE, ADSL, or VDSL as the access type. If you selected MPLS as the link type, you can select Ethernet (default) or LTE as the access type. <p>You can select the LTE, ADSL, or VDSL access type for only one WAN link.</p>	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
PPPoE/PPP	<p>By default, this toggle button is disabled. Click the toggle button to enable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet) or PPP (Point-to-Point Protocol).</p> <p>PPPoE works with Ethernet, ADSL, and VDSL access types. PPP works with the LTE access type.</p> <p>NOTE: This toggle button is not available for Internet links with LTE as the access type.</p> <p>If you enable this toggle button, you must specify the PPPoE or PPP parameters (username, password, and authentication protocol) for the PPPoE or PPP server, respectively. The PPPoE or PPP server assigns an IP address to the WAN link after successful authentication. For more information, see the <i>PPPoE/PPP Settings</i> section in this table.</p> <p>If you have disabled this toggle button, select a method (DHCP or STATIC) to assign an IP address to the WAN link from the Address Assignment list.</p>	<ul style="list-style-type: none"> Secure SD-WAN Advanced
Egress Bandwidth	<p>Enter the maximum bandwidth (in mega bits per second [Mbps]) to be allowed for the WAN link. Range: 1 through 10,000</p> <p>NOTE: This option is not available for Internet and MPLS links with LTE access type.</p>	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Underlay Address Families		
Address Assignment	<p>Select the method for IP address assignment. The options available are:</p> <ul style="list-style-type: none"> DHCP—Select DHCP to assign IP address by using a DHCP server. STATIC—Select STATIC to assign a static IP address. 	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Advanced Settings		

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Underlay Address Family		
Provider	Enter the name of the service provider who is responsible for providing the WAN link.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Cost/Month	<p>Enter the cost for using the WAN link per month and select the currency in which the cost is indicated from the adjacent drop-down list.</p> <p>Range: 1 through 10,000.</p> <p>In bandwidth-optimized SD-WAN, CSO uses this information to identify the least expensive link to route traffic when multiple WAN links meet SLA profile parameters.</p>	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Enable Local Breakout	Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Breakout Options	Select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Autocreate Source NAT Rule	Click the toggle button to enable or disable the automatic creation of source NAT rules. By default, this field is enabled when local breakout is enabled on the WAN link.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Translation	<p>Select the type of NAT to use for the traffic on the WAN link:</p> <ul style="list-style-type: none"> Interface—Use interface-based NAT, which is the default option. Pool—Use pool-based NAT. If you select this option, you must specify the IP addresses that can be used for the NAT pool. <p>NOTE: No NAT is performed for tenant-owned public IP addresses.</p>	<ul style="list-style-type: none"> Secure SD-WAN Advanced

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the most preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
BGP Underlay Options	<p>NOTE: This setting can be configured only if the address assignment is static and local breakout is enabled.</p> <p>Click the toggle button to enable BGP underlay routing.</p> <p>When you enable BGP underlay routing, route advertisements to the primary PE node and, if configured, the secondary PE node occur as follows:</p> <ul style="list-style-type: none"> CSO advertises the WAN interface subnet. If you configured pool-based translation, CSO advertises the NAT address pool. <p>NOTE: If underlay BGP is enabled for a WAN link, then the routes learnt from BGP are installed for local breakout; CSO does not generate the static default route.</p>	<ul style="list-style-type: none"> Secure SD-WAN Advanced
Use For Fullmesh	Click the toggle button to specify that the WAN link is part of a fullmesh topology.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Mesh Overlay Link Type	<p>When Use for Fullmesh field is enabled, select the type of mesh overlay link—GRE and GRE_IPSEC.</p> <p>If the link type is Internet, by default, the value for mesh overlay link type is GRE_IPSEC.</p> <p>If the link type is MPLS, select one of the following options:</p> <ul style="list-style-type: none"> GRE-IPSEC GRE 	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Mesh Tag	<p>When the Use for Fullmesh field is enabled, enter the tag to be associated with the WAN link for creating tunnels. You can assign only one tag to the link.</p> <p>Matching mesh tags is one of the criteria used to form tunnels between sites that support meshing.</p> <ul style="list-style-type: none"> • For a branch site, you can select one mesh tag. • For an enterprise hub, you can select one or more mesh tags. <p>For more information about mesh tags, see “Mesh Tags Overview” on page 240.</p>	<ul style="list-style-type: none"> • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Connects To Hub	<p>Click the toggle button to specify that the WAN link of the site connects to a hub.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted. • For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted. 	<ul style="list-style-type: none"> • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Backup Link	<p>Select a backup link through which traffic can be routed when the primary (other) links are unavailable. You can select any link other than the default links or links that are configured exclusively for local breakout traffic.</p>	<ul style="list-style-type: none"> • Secure SD-WAN Essentials • Secure SD-WAN Advanced
Default Link	<p>Select one or more links to be used for routing traffic in the absence of matching SD-WAN policies.</p> <p>A site can have multiple default links to the hub site. If a site has more than one default link, equal-cost multipath (ECMP) is used to balance the traffic between the links.</p>	<ul style="list-style-type: none"> • Secure SD-WAN Essentials • Secure SD-WAN Advanced
VLAN ID	<p>Enter the VLAN ID that is associated with the data link. A data VLAN identifier is an integer.</p> <p>Range: 0 through 65,535</p>	<ul style="list-style-type: none"> • Secure SD-WAN Essentials • Secure SD-WAN Advanced
WAN_1 (WAN-Interface-Name)	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN_1 link is disabled.</p> <p>Refer to the fields described for WAN 0 for an explanation of the fields.</p>	<ul style="list-style-type: none"> • Secure SD-WAN Essentials • Secure SD-WAN Advanced

Table 40: Fields on the Add Site Template Page (continued)

Field	Description	Applicable To
WAN_2 (WAN-Interface-Name)	Click the toggle button to enable or disable this WAN link. By default, the WAN_2 link is disabled. Refer to the fields described for WAN 0 for an explanation of the fields	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
WAN_3 (WAN-Interface-Name)	Click the toggle button to enable or disable this WAN link. By default, the WAN_3 link is disabled. Refer to the fields described for WAN 0 for an explanation of the fields	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Advanced Configuration		
OAM IP Prefix	Enter an IPv4 address prefix for the loopback interface on the CPE device. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network. NOTE: We recommend that you do not configure this setting (leave the IP Prefix field blank) because management connectivity is handled automatically by CSO.	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
DVPN Threshold for Tunnel Creation	Specify the minimum number of sessions that should be closed in two minutes to automatically trigger a tunnel creation. When the number of sessions closed exceeds the specified threshold, a tunnel is created between the branch site and the destination site.	<ul style="list-style-type: none"> Secure SD-WAN Advanced
DVPN Threshold for Tunnel Deletion	Specify the maximum number of tunnels that should be closed in 15 minutes to trigger a tunnel deletion. When the number of sessions closed is lower than the specified threshold, the tunnel between the branch site and destination site is deleted.	<ul style="list-style-type: none"> Secure SD-WAN Advanced

Table 40: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
LAN Segment Configuration	<p>Displays the VLANs and their IDs that you configure on the device.</p> <ul style="list-style-type: none"> Optional: To add a VLAN, click the + icon on the top right corner of the LAN Segments table. The Create LAN Segment page appears. See Table 41 on page 237 to complete the configuration. To edit details of a VLAN, select the VLAN and click the Edit icon (pencil) on the top right corner of the LAN Segments table. The Edit LAN Segment page appears, displaying the same fields that are presented when you add a VLAN. <p>Modify the parameters as needed and click OK. The changes that you made for the LAN segment are saved and the updated parameters appear on the LAN Segments table.</p> <ul style="list-style-type: none"> To delete one or more VLANs, select the VLANs and click the Delete icon on the top right corner of the LAN Segments table. 	<ul style="list-style-type: none"> Secure SD-WAN Essentials Secure SD-WAN Advanced
Additional Configuration		
Configuration Templates (Optional)	<p>Select one or more configuration templates from the list. This list is filtered based on the device that you select.</p> <p>Configuration templates are stage-2 templates that are added by your OpCo administrators or SP administrators or Tenant administrators.</p> <p>NOTE: You must set the parameters of the configuration templates that you have selected before you move to the LAN section.</p> <p>To set the parameters for the selected configuration templates:</p> <ol style="list-style-type: none"> After you select one or more configuration templates, click Set Parameters. <p>The Device Configurations page appears. This page consists of two tabs—Configure and Summary.</p> <ol style="list-style-type: none"> In the Configure tab, enter values for the parameters in each configuration templates. <p>(Optional) View the CLI commands in the Summary tab.</p> <ol style="list-style-type: none"> Click OK. <p>You have added and set the parameters for the configuration templates that are part of the site template that you are creating.</p>	<ul style="list-style-type: none"> Device Management Security Services Secure SD-WAN Essentials Secure SD-WAN Advanced

Table 41: Fields on the Add LAN Segment Page

Field	Description
Add LAN Segment	
Use for Overlay VPN	<p>When this option is enabled, the LAN segment is associated with the selected department (VRF + ZONE) for overlay traffic to other sites.</p> <p>When this option is disabled, the LAN segment is attached to the security zone for underlay breakout. Zone-based security policies must be defined by the user.</p>
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
CPE Port	Select the CPE device port.
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 1 through 4049.</p>
Use for Native VLAN	When this option is enabled, the VLAN ID is used for untagged traffic. The selected interface is configured with native-vlan-id equal to the number specified for the VLAN ID.
Department	<p>Select a department to which the LAN segment is to be assigned.</p> <p>Alternatively, click the Create Department link to create a new department and assign the LAN segment to it. See “Add a Department” on page 783 for details.</p> <p>You group LAN segments as departments for ease of management and for applying policies at the department-level.</p>
Gateway Address/Mask	Specify a unique and valid IPv4 address with subnet mask (for example, 10.0.2.1/24). This address is the default gateway for endpoints in this LAN segment. Configuration of LAN subnets in the range 100.112.0.0 - 100.127.255.255 is not supported.
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP. DHCP is disabled by default.</p> <p>You enable DHCP if you want to assign IP addresses by using a DHCP server. You disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p>NOTE: If you enable DHCP, fields related to DHCP-related parameters are displayed. You must configure the fields.</p>

RELATED DOCUMENTATION

[About the Site Templates Page | 219](#)

[Cloning, Editing, and Deleting Site Templates | 221](#)

[Add Branch Sites by Using a Site Template | 220](#)

Adding and Configuring Sites by Importing a JSON File

You can add and configure one or more sites in CSO by uploading a JavaScript Object Notation (JSON) file that contains the parameters for adding and configuring the sites.

Before you begin, ensure that the JSON file contains all the parameters required for each site that you want to add or configure.

NOTE: We recommend that you create the JSON file by referring to the sample JSON file provided by CSO. Refer to Step 3 of the procedure for downloading and modifying the sample JSON file.

To add and configure multiple sites by uploading a JSON file:

1. Click **Resources > Site Management**.

The Sites page appears.

2. Click **More** and select **Import Sites**.

The **Import Sites** page appears.

3. (Optional) Download a sample JSON file by clicking the **Download Sample JSON** link. Edit the parameters based on your requirements and save the file.

4. Click **Browse** and navigate to the directory that contains the JSON file.

5. Select the file and click **Open**.

6. Click **Import**.

A message is displayed indicating that the file is imported to CSO. After the file is imported to CSO successfully, you are returned to the Sites page, where you can view the newly added sites:

- If you enabled automatic activation for the sites, CSO activates the sites.

If you selected a service while adding the sites, then CSO provisions the sites and the status of the sites changes to PROVISIONED. If you did not select a service, then the status of the sites changes to MANAGED. You can edit the sites to add the service. After you add the service, CSO applies the service provisioning configuration and the sites are provisioned.

- If you did not enable automatic activation, CSO sets the status of the sites to CONFIGURED. You must manually activate the sites after which CSO provisions the sites. See [“Activate a Device” on page 252](#) or [“Activating Dual CPE Devices \(Device Redundancy\)” on page 255](#).

After the sites are activated and provisioned, you can install certificates and create policies for the sites. See the *Managing Policies, Profiles, and Proxies* section in this guide for details.

RELATED DOCUMENTATION

[About the Site Management Page | 68](#)

[Manually Adding Branch Sites | 119](#)

Managing Mesh Tags

IN THIS CHAPTER

- [Mesh Tags Overview | 240](#)
- [About the Mesh Tags Page | 241](#)
- [Creating User-defined Mesh Tags | 242](#)

Mesh Tags Overview

A mesh tag is a label that you associate with a WAN link of a spoke site. Mesh tags provide you the flexibility to establish overlay tunnels between WAN links of two different spoke sites. If WAN links are associated with same mesh tags, CSO creates a VPN tunnel between WAN links of spoke sites (enterprise hub to enterprise hub, branch site to enterprise hub, branch site to branch site).

NOTE: Mesh tags are applicable only for SD-WAN sites in the Real-time optimized mode (Full mesh).

Mesh tags can be predefined (MPLS and Internet) or user-defined. You can create user-defined mesh tags on the **Administration > Mesh Tags** page.

NOTE: With mesh tags, you can connect two WAN links even if the link types (MPLS and Internet) are different.

For example, consider that a tenant has two sites—Site A and Site B. Site A has four WAN links (WAN_A0 through WAN_A3) and Site B has three WAN links (WAN_B0 through WAN_B2). WAN_A0 and WAN_B0 are associated with MPLS (predefined mesh tag), and WAN_A1 and WAN_B1 are associated with Internet (predefined mesh tag).

A tunnel is established between WAN-A0 and WAN-B0 because they are associated with the same predefined mesh tags.

NOTE: You can associate mesh tags for up to three WAN links.

RELATED DOCUMENTATION

[About the Mesh Tags Page | 241](#)

[Creating User-defined Mesh Tags | 242](#)

About the Mesh Tags Page

To access this page, select **Resources > Mesh Tags** in Customer Portal.

Use this page to view predefined mesh tags and create user-defined mesh tags. Mesh tags connect WAN links of different sites. CSO creates a tunnel between WAN links if they are associated with the same mesh tag (user-defined or predefined).

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a mesh tag—See [“Creating User-defined Mesh Tags” on page 242](#).
- Delete a mesh tag. Select a mesh tag and click the delete icon.

Field Descriptions

[Table 42 on page 241](#) describes the fields on the Mesh Tags page.

Table 42: Fields on the Mesh Tag Page

Field	Description
Name	Displays the name of the mesh tag.
Tenant	Displays the tenant name to which the site is associated.
Type	Displays whether the mesh tag is a predefined or a user-defined.

RELATED DOCUMENTATION

| [Mesh Tags Overview](#) | 240

Creating User-defined Mesh Tags

CSO creates a tunnel between WAN links of two different sites if they are associated with the same mesh tag (user-defined or predefined).

To create a user-defined mesh tag:

1. Select **Resources > Mesh Tags**.

The Mesh Tags page appears.

2. Click the add icon (+) to create a mesh tag.

The Create New Mesh Tag page appears.

3. Complete the configuration according to the guidelines provided in [Table 43 on page 242](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to save the changes.

The user-defined mesh tag is created.

If you want to discard your changes, click **Cancel** instead.

Table 43: Fields on the Create New Mesh Tag Page

Field	Description
Name	Enter a unique name for the mesh tag.
Description	Enter a description for the mesh tag.

RELATED DOCUMENTATION

| [About the Mesh Tags Page](#) | 241

Managing Dynamic Mesh

IN THIS CHAPTER

- [Dynamic Mesh Tunnels Overview | 243](#)
- [Adding On-Demand Mesh Tunnels | 244](#)
- [Deleting On-Demand Mesh Tunnels | 246](#)

Dynamic Mesh Tunnels Overview

In releases earlier than CSO 4.1.0, all the overlay tunnels for the site are established between branch sites during the Zero Touch Provisioning (ZTP) process.

However, starting with CSO Release 4.1.0, during ZTP, only the following static tunnels are established:

- Between a branch site and the corresponding enterprise hub (primary enterprise hub or secondary enterprise hub)
- Between a branch site and the provider hub (primary provider hub or secondary provider hub)
- Between two enterprise hubs

Therefore, the communication between two branch sites (with SD-WAN Advanced service) is established only through the enterprise hub or the provider hub.

For sites with SD-WAN Advanced service, CSO dynamically creates or deletes a mesh tunnel (also called DVPN tunnel) between two branch sites directly so that the traffic does not go through an enterprise hub or a provider hub, if:

- The number of sessions closed between two branch sites crosses the configured threshold value, and
- The WAN links of branch sites have matching mesh tags. For more information, see [“Mesh Tags Overview” on page 240](#).

NOTE: The dynamic mesh feature is applicable only for SD-WAN Advanced sites (Full mesh).

Sites with SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or the Tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.

The tenant administrator can modify the default threshold value on the following pages:

- The **Administration > Tenant Settings** page (Dynamic Mesh section) of Customer Portal (global level)
- The Add Branch Site page
- The Add Enterprise Hub page

The threshold value that you specify at site-level takes precedence over the global-level threshold values.

That is, the threshold value that you specify on the Add Site page (branch or enterprise hub) overrides the threshold value that you specified on the Tenant Settings page of Customer Portal.

CSO allows you to manually create or delete dynamic mesh tunnels between a source site and a destination site by using the Add On-Demand Mesh Tunnel or Delete On-Demand Mesh Tunnel pages in Customer Portal.

From Release 5.1.0 onward, CSO supports site-to-site tunnels for WAN links of CPE devices behind NAT in full mesh topology. In releases before Release 5.1.0, CSO supports private IP addresses for WAN links behind NAT only for the WAN links that are not selected for meshing, and such WAN links can establish the tunnels only to provider hubs. The support for CPE devices behind NAT in full mesh topology is applicable only for spoke devices. The OAM hubs, data hubs, and enterprise hubs or on-premise gateways require static public IP addresses for their WAN interfaces.

RELATED DOCUMENTATION

[View and Edit Tenant Settings](#) | 27

Adding On-Demand Mesh Tunnels

An OpCo administrator or the Tenant administrator can create a mesh tunnel between a source site and destination site by using the CSO GUI in Customer Portal.

To create a mesh tunnel between the source site and a destination site:

1. Select **Resources > Site Management**.

The Sites page appears.

2. Click the site to which you want to add mesh tunnels.

The *Site Name* page appears.

3. On the WAN > Overlay tab, click +.

The Add Dynamic Mesh Tunnel page appears.

4. Complete the configuration according to the guidelines [Table 44 on page 245](#).

5. Click **Ok** to save the changes. If you want to discard the changes, click **Cancel** instead.

A tunnel is created between the source site and a destination site.

Table 44: Fields on On-demand VPN Tunnel page

Field	Description
Add Tunnel Threshold	
Source Site	Displays the name of the source site.
Destination Site	Select the destination site from the list.
Delete Tunnel	
Displays the threshold value (sessions closed) below which a tunnel is deleted between two sites.	
NOTE: Sites with SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or a tenant administrator can create a static tunnel between a source site and destination site.	
Enable Threshold	By default, this toggle button is disabled. That is, even if the threshold value (sessions closed) is met, CSO does not delete mesh tunnels. You have to manually delete the mesh tunnel that you created.
Sessions Closed	Displays the number of sessions closed for 15 minutes.

RELATED DOCUMENTATION

| [Dynamic Mesh Tunnels Overview](#) | 243

Deleting On-Demand Mesh Tunnels

A user with either OpCo administrator or Tenant administrator roles can delete a VPN tunnel between a source site and destination site by using the CSO GUI in Customer Portal.

To delete a mesh tunnel between a source site and a specific destination site:

1. Select **Resources > Site Management**.
The Sites page appears.
2. Click the site from which you want to delete mesh tunnels.
The *Site Name* page appears.
3. On the WAN tab, click **+**.
The Delete On-Demand Mesh Tunnel page appears.
4. Complete the configuration according to the guidelines [Table 45 on page 246](#).
5. Click **Ok** to save the changes. If you want to discard the changes, click **Cancel** instead.

A VPN tunnel is deleted between the source site and a specific destination site.

Table 45: Fields on the Delete On-Demand Mesh Tunnel page

Field	Description
Delete Tunnel Threshold	
Source Site	Displays the name of the source site.
Destination Site	Select the destination site from the list.
Delete Tunnel	
Displays the threshold value (sessions closed) below which a tunnel is deleted between two spokes.	

Table 45: Fields on the Delete On-Demand Mesh Tunnel page *(continued)*

Field	Description
Enable Threshold	By default, this toggle button is disabled. That is, even if the threshold value (sessions closed) is met, CSO does not create mesh tunnels. You have to manually create the mesh tunnel that you deleted.
Sessions Closed	Displays the number of sessions closed for 2 minutes. .

RELATED DOCUMENTATION

[Dynamic Mesh Tunnels Overview](#) | 243

3

PART

Managing Devices and Resources

Managing Devices | **249**

Managing Device Images | **266**

Managing Resources | **269**

Managing Device Templates | **332**

Managing Configuration Templates | **351**

Managing Licenses | **401**

Managing Signature Database and Certificates | **409**

Managing Juniper Identity Management Service | **430**

Managing Devices

IN THIS CHAPTER

- [Device Redundancy Support Overview | 250](#)
- [Activate a Device | 252](#)
- [Activating Dual CPE Devices \(Device Redundancy\) | 255](#)
- [Viewing the History of Tenant Device Activation Logs | 257](#)
- [Zero Touch Provisioning Overview | 259](#)
- [Workflow for Onboarding a Device Using ZTP | 262](#)
- [Configure an SRX Series CPE to Discover an EX Series Switch or AP Connected to the CPE | 265](#)

Device Redundancy Support Overview

Contrail Service Orchestration (CSO) provides support for spoke device redundancy for large enterprise SD-WAN branch sites. You can configure an SD-WAN site with two CPE devices to act as primary and secondary devices and protect the site against device and link failures. If the primary device fails, the secondary device takes over the traffic processing.

NOTE: You must use the same device model for both primary and secondary devices and the devices must have the same version of Junos OS installed.

The following SD-WAN features are not supported for device redundancy:

- LTE WAN backup link
- Service chain support

NOTE: Device redundancy is supported only on SD-WAN deployments.

Prerequisites for SRX Series Devices

The prerequisites to configure an SD-WAN site with dual CPE SRX Series devices are as follows:

- For SRX Series, you need to form the cluster manually by connecting two SRX Series devices together using a pair of the same type of Ethernet connections. To create an SRX cluster, see [Chassis Cluster Feature Guide for SRX Series Devices](#).
- Log in to any one of the SRX Series devices, copy the **Stage-1** configuration from the **Sites** page and paste it into the console screen and commit the configuration.

Supported Connection Plans

The following connection plans are supported for device redundancy:

- Dual NFX250 as SD-WAN CPEs—Supports dual CPE NFX Series devices on an SD-WAN site.
- Dual SRX as SD-WAN CPEs—Supports dual CPE SRX Series devices on an SD-WAN site.
- Dual SRX4x00 as SD-WAN CPEs—Supports SRX 4100, SRX4200, and SRX4600 devices as dual CPE devices in an SD-WAN site.

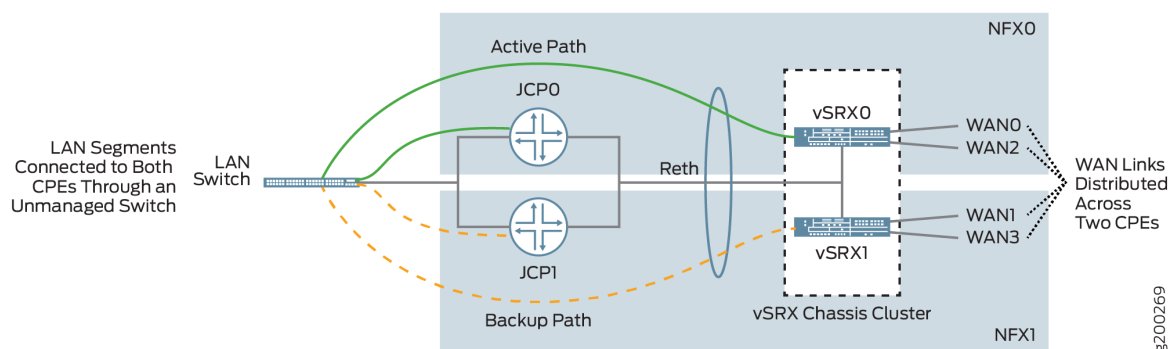
Create and Configure an SD-WAN Site

You can create and configure an SD-WAN site with dual CPE devices and the two devices back up each other, with one node acting as the primary device and the other as the secondary device. The workflow to add and configure a site with dual CPE devices is similar to the single CPE device. For more information about creating and configuring a site with dual CPE devices, see [“Add a Branch Site with SD-WAN Capability” on page 120](#).

Dual CPE Devices Logical Topology for NFX Network Services Platform

[Figure 12 on page 251](#) shows the logical topology of the NFX Series dual CPE devices.

Figure 12: Dual CPE Device Topology - NFX Network Services Platform



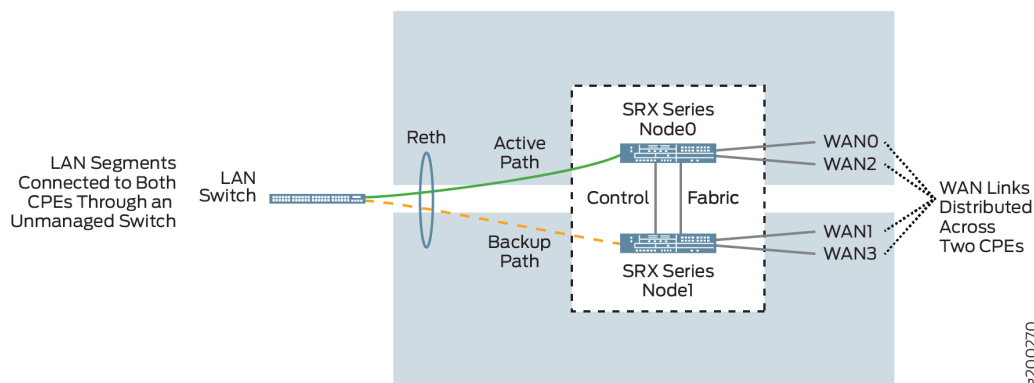
You can form a cluster using two NFX Series devices. The front panel ports of the NFX Series devices are used to interconnect two NFX Series devices and to carry the control and fabric interconnect traffic between the two NFX250 devices.

The Junos Control Plane (JCP) component acts as a switch, controls the front panel ports, and sends the traffic which arrives from the LAN or WAN to the NFX Series devices. On the LAN, the active/backup mechanism is used and if the primary device fails, the secondary device takes over processing of traffic. On the WAN, the active/active mechanism is used and all four WAN links are active and distributed across two NFX Series devices.

Dual CPE Devices Logical Topology for SRX Series Gateway Devices

[Figure 13 on page 252](#) shows the logical topology of the SRX Series dual CPE devices.

Figure 13: Dual CPE Device Topology - SRX Series Devices



You can form a cluster using two SRX devices. A chassis cluster is formed between these nodes and performs as a single logical router. On the LAN, the active/backup mechanism is used and if the primary device fails, the secondary device takes over traffic processing. On the WAN, the active/active mechanism is used and all four WAN links are active and distributed across two SRX Series devices.

RELATED DOCUMENTATION

[Add a Branch Site with SD-WAN Capability | 120](#)

[Activating Dual CPE Devices \(Device Redundancy\) | 255](#)

Activate a Device

IN THIS SECTION

- [Manually Activate a Device That Supports Phone-Home Client | 253](#)
- [Manually Activate a Device That Does Not Support Phone-Home Client | 254](#)

If the automatic activation of a site is disabled, you must manually activate the device that is associated with the site. Use the following procedures (as applicable) to manually activate CPE devices, enterprise hub devices, and cloud spoke devices.

To activate dual-CPE devices, see [“Activating Dual CPE Devices \(Device Redundancy\)” on page 255](#).

NOTE:

You can manually activate a device only when:

- The status of the site (with which the device is associated) is Configured.
- The management status of the device is Device_Detected or Device_Connected.

Manually Activate a Device That Supports Phone-Home Client

If a device supports the phone-home client, the ZTP toggle button is enabled by default in the corresponding device template.

To manually activate a device that supports the phone-home client:

1. Do one of the following:

- a. Select **Resources > Devices**.

The Devices page appears.

- b. Select the device that you want to activate and click **Activate Device**.

The **Activate Device** page appears. The Activate Device page consists of the Device Information and Device Activation tabs. Proceed to step 2.

- a. Select **Resources > Site Management**.

The Sites page appears.

- b. Click the **Site-Name** link for the site with which the device is associated.

The **Site-Name** page appears.

- c. On the **Devices** tab, select the device that you want to activate and click **Activate Device**.

The **Activate Device** page appears. The Activate Device page consists of the Device Information and Device Activation tabs.

2. On the Device Information tab, enter the activation code for the device in the **Activation Code** field.

The activation code that you enter must match the activation code that is provided during the site addition workflow.

3. Click **Next**.

The Device Activation tab appears displaying the progress of the device activation.

4. After the device is activated, click **OK**.

The Sites page appears. If the device is successfully activated, the Management Status of the device and site changes to **MANAGED**. The status of the device and site changes to **PROVISIONED** only after the Security or SD-WAN service is applied.

Manually Activate a Device That Does Not Support Phone-Home Client

If the device does not support the phone-home client, you must push the stage-1 configuration to the device manually from the Devices page and then manually activate the device.

To push the stage-1 configuration manually:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select the device and click **Stage1 Config**.

The **Copy the following config and deploy it to the device** page appears.

3. Click **Copy**.

A confirmation message appears indicating that the stage-1 configuration is copied to the clipboard.

4. Log in to the device console and enter the Junos OS configuration mode.

5. Paste and then, commit the configuration.

The Management Status of the device on the Devices page changes to **Device_Detected**.

6. Proceed to activate the device. The rest of the workflow is the same as the one you encounter when you manually activate a device that supports the phone-home client. Refer to the [“Manually Activate a Device That Supports Phone-Home Client” on page 253](#) for details.

RELATED DOCUMENTATION

[Activating Dual CPE Devices \(Device Redundancy\) | 255](#)

[Zero Touch Provisioning Overview | 259](#)

Activating Dual CPE Devices (Device Redundancy)

You can activate a device after the device status is changed to **EXPECTED** in the Sites page. When you see the device status is **EXPECTED**, it indicates that the device is ready to be activated. If you see the device status as **Undefined**, contact your service provider for assistance.

NOTE: You must activate both the primary and the secondary devices simultaneously.

You must use the same device model for both primary and secondary devices and the devices must have the same version of Junos OS installed.

You can manually activate a device only when:

- The status of the site (with which the device is associated) is Configured.
- The management status of the device is Device_Detected or Device_Connected.

To activate dual CPE devices used as a cluster:

1. Log in to Customer Portal.

2. Select **Resources > Site Management**.

The Site Management page appears.

3. Click on the *Site Name*.

The *Site Name* page appears.

4. On the **Devices** tab, select the cluster device, and click **Activate Device**.

The Activate Device page appears. The Activate Device page consists of Device Information and Device Activation tabs.

NOTE: You can also activate the device from the **Resource > Devices** page.

5. On **Device Information** page, complete the configuration according to the guidelines provided in [Table 46 on page 256](#).

Table 46: Fields on the Activate Device Page

Field	Description
Site Name & Type	View the name of the site on which the CPE device is activated.
Connected Region	View the name of the region to which the CPE device is connected.
Primary Device Serial Number	View the serial number of the primary CPE device.
Primary Device Activation Code	Enter the activation code of the primary device that your service provider supplied for the device.
Secondary Device Serial Number	View the serial number of the secondary CPE device.
Secondary Device Activation Code	Enter the activation code of the secondary device that your service provider supplied for the device.

6. Click **Next**.

The Activate Device page appears displaying the progress of the device activation.

7. After the activation process is complete, click **OK**.

The *Site Name* page appears. If the device activation is successful, the management status of the cluster device changes to **MANAGED**. If you have selected a service while adding the device, then CSO generates the service provisioning configuration and applies it on the device. The status of the device changes to **PROVISIONED**.

RELATED DOCUMENTATION

[Device Redundancy Support Overview | 250](#)

[Activate a Device | 252](#)

[About the Site Management Page | 68](#)

[Add a Branch Site with SD-WAN Capability | 120](#)

[About the Certificates Page | 417](#)

Viewing the History of Tenant Device Activation Logs

You can use the Activation Logs page to view the history of device activation logs. You can also view the details of the activation logs and their status.

To view the tenant device activation logs:

1. Click **Resources > Tenant Devices**.

The Tenant Devices page appears, which list all devices.

2. Select a device and click **More > Activation Logs**.

The Activation Logs page is displayed. [Table 47 on page 257](#) describes the fields on the Activation Logs page.

3. Click a task name.

The ZTP Logs page appears. [Table 48 on page 258](#) describes the fields on the ZTP Logs page.

4. Click the Task Name.

The Job Status page appears. [Table 49 on page 258](#) describes the fields on the Job Status page.

5. Click **OK** to return to the previous page.

Table 47: Fields on the ZTP History Page

Field	Description
In progress	View the number of activated tasks that are in progress.
Success	View the number of activated tasks that are successful.
Failure	View the number of activated tasks that have failed.
Name	View the name of the task. Example: csp.tssm_ztp-Juniper-site-17-NFX-250-8052cc9451914be28c7c98fb64fd0db3
Start Date	View the start date and time of the task.
End Date	View the end date and time of the task.

Table 47: Fields on the ZTP History Page (*continued*)

Field	Description
Status	View the status of the task to know whether the task succeeded or failed.
Log	View the import logs. Click a log to access more detailed information about the imported log.

Table 48: Fields on the ZTP Logs Page

Field	Description
Task Name	View the ID created for the task. Example: install-license-to-device
Status	View the status of the task to know whether the task succeeded or failed.

Table 49: Fields on the Job Status Page

Field	Description
Name	View the name of the task.
Actual Start Time	View the start date and time of the task.
User	View the name of the user who activated the task.
End Time	View the end date and time of the task.
State	View the status of the task to know whether the task succeeded or failed.

RELATED DOCUMENTATION

| *About the Tenant Devices Page*

Zero Touch Provisioning Overview

Zero Touch Provisioning (ZTP) enables you to configure and provision devices automatically, and thus reduces the manual intervention required for adding devices to a network.

Starting from CSO Release 6.0.0, the ZTP process is simplified to provide more flexibility and enable faster deployment of devices in a network. The device management and service provisioning processes are separated, thus reducing the time required for CSO to onboard and manage a device. For branch and enterprise hub devices, you can choose to either onboard a device with a service configured on it or configure the service later.

Additionally, ZTP supports automatic formation of an SRX chassis cluster during the onboarding process. You can now onboard a cluster without manually configuring each node on a cluster.

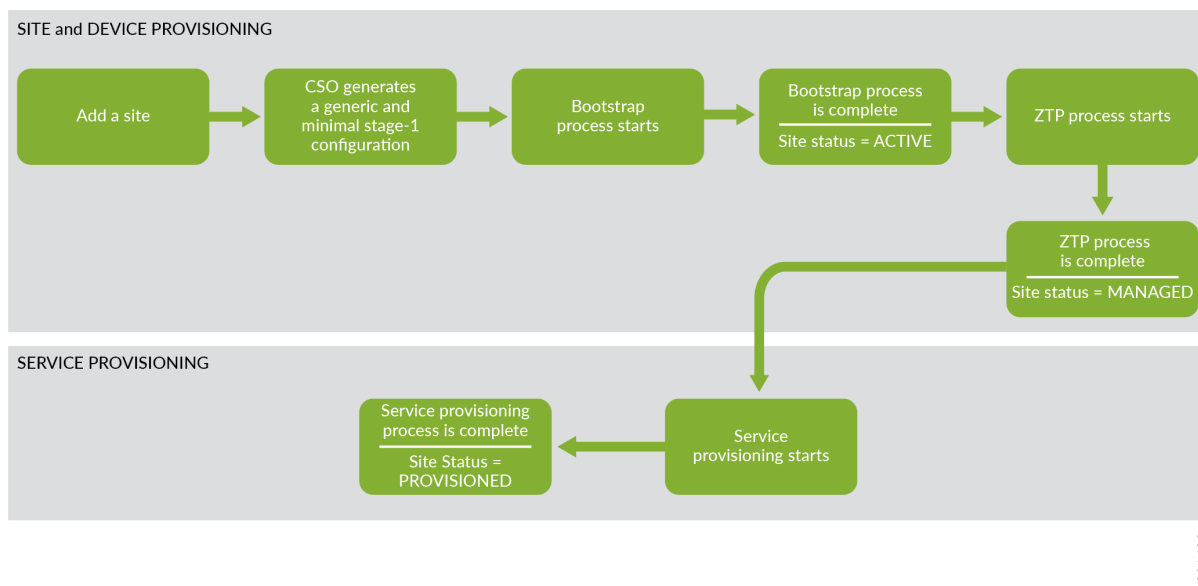
The following are the options available for onboarding a device:

- **Device Management**—Enables you to onboard a device without specifying any service in a branch or an enterprise hub site. The device is connected to and managed by CSO. After the device is added, you can edit the site at any time to add the service. The Device Management option is selected by default. You cannot disable this option.
- **Security Services**—Provides next-generation firewall (NGFW) services. This option is available only for branch sites.
- **Secure SD-WAN Essentials**—Provides basic SD-WAN services.
- **Secure SD-WAN Advanced**—Provides complete SD-WAN services, which includes Secure SD-WAN Essential services.

For more information about SD-WAN Essentials and Advanced services, see *SD-WAN Overview*.

[Figure 14 on page 260](#) provides a brief description of the simplified ZTP process.

Figure 14: Simplified ZTP Process



Simplified ZTP involves the following high-level steps:

1. CSO activates the device that is associated with the site.
2. CSO establishes a management connection (outbound SSH) with the device.
3. CSO applies the stage-1 configuration (including the device configuration) and the status of the device changes to Managed state. The device can remain in the Managed state for any duration. You can perform the following tasks when the device is in the Managed state:
 - Apply stage-2 configuration or configuration templates
 - Access the device console
 - Reboot the device
 - Install licenses, certificates, and application signatures
 - RMA the device
4. CSO generates the service provisioning configuration and applies it on the device if you selected a service (Security Services or SD-WAN) while adding the device. The site status shows Provisioned only after the service is applied successfully.

Devices Supported

You can provision the following devices (including dual CPE devices, if applicable), by using the simplified ZTP process:

- NFX150
- SRX300, SRX320, SRX340, SRX345, SRX380, SRX550 High Memory (SRX550M), SRX4100, SRX4200, SRX4600, and SRX1500
- vSRX on an x86 server
- Dual CPEs (SRX devices)

Benefits

The simplified ZTP process offers the following benefits:

- Simplified, faster, and automated deployment of configurations.
- Quick access and remote management of the device.
- Auto-generated configurations that are more accurate.
- Faster scaling of the network because you need not manually apply configuration on each device in the network.
- Automated cluster configuration for SRX devices on branch and enterprise hub sites.
- Enhanced monitoring and troubleshooting.

RELATED DOCUMENTATION

| [Workflow for Onboarding a Device Using ZTP](#) | 262

Workflow for Onboarding a Device Using ZTP

This topic provides the steps that you need to perform for successfully onboarding a device to the network by using ZTP:

Prerequisites:

The following prerequisites are necessary for ZTP:

- The device must have connectivity to CSO and the phone-home server (<https://redirect.juniper.net>). Use telnet to verify connectivity:
 - For phone-home server: **telnet redirect.juniper.net:443**
 - For CSO: **telnet CSO Hostname/IP:443**

If the connection is established, the device has connectivity to the phone-home server and CSO.

- The required certificates for phone-home server and CSO are present on the device.
1. From Customer Portal, add a branch site or an enterprise site, and associate a device.

You can choose one of the following options:

- Add the site without specifying any services
- Add the site with services
- Add the site and specify the services later

NOTE: You cannot add a cloud spoke site without specifying a service.

For information about adding a branch site, see:

- [“Add a Branch Site with SD-WAN Capability” on page 120.](#)
- [“Add a Standalone Next-Generation Firewall Site” on page 153.](#)

For information about adding an enterprise hub, see [“Add Enterprise Hubs with SD-WAN Capability” on page 76.](#)

2. Activate the device:

- If you have enabled the **Auto Activate** field while adding a branch site or an enterprise hub, ZTP of the device is automatically triggered after the site is added to CSO.
- If you have disabled the **Auto Activate** field while adding a branch site or an enterprise hub, you must manually activate the device.

To manually activate the device:

- a. Select **Resources > Site Management**.

The Site Management page appears.

- b. On the Site Management page, click the site that you want to activate.

The detailed view of the site appears.

NOTE: You can activate a site that is in the CONFIGURED state.

- c. Click the **Devices** tab.

- d. Select the device that you added to the site and click **Activate Device** to activate the device.

The Activate Device page appears.

- e. On the Activate Device page, enter the activation code for the device. The activation code must match the activation code that you provided during the site addition workflow.

- f. Click **Next**.

The progress of device activation is displayed.

- g. After the device is activated, click **OK**.

The Sites page appears.

- If you have to activate vSRX or SRX4X00 Services Gateway devices:

- a. Select **Resources > Site Management**.

The Sites page appears.

- b. Click on the site that you want to activate.

The *Site-Name* page appears.

- c. On the Devices tab, select the device that you want to activate and click **Stage1 Config**.

A new page appears that displays the stage-1 configuration of the device.

- d. Click **Copy to Clipboard** to copy the stage-1 configuration of the device.

- e. Log in to the CLI of the device and enter the configuration mode.
- f. Paste the stage-1 configuration and commit.

The activation process includes the following tasks:

- CSO first models the site and generates the stage-1 configuration.
- The device connects to CSO through the phone-home client (PHC) to the Redirect Server, which authenticates the device.
- Based on the device serial number, the Redirect Server provides the CSO certificate and CSO host name to the device.
- The device establishes an outbound SSH connection with CSO.
- CSO applies the pre-scripts and stage-1 configuration (includes the device configuration).
- The status of the device changes to MANAGED.
- If you selected a service (security services or SD-WAN) while adding the device, then CSO generates the service provisioning configuration and applies it on the device to make it functional and ready for the intended functionality. The device is provisioned only after the service is applied.

If you did not select a service while adding the device, then the device remains in the MANAGED state until you apply the service. You can edit the site and add the service. After you add the service, CSO applies the service provisioning configuration and the device is provisioned.

For additional functionality, you can create a stage-2 template and apply the template on the device. For example, the stage-2 template can include LAN configuration, firewall policies, and so on.

Use the Jobs page (**Resources > Monitor > Jobs**) to view the bootstrap logs, ZTP logs, and service provisioning logs. If any of the tasks (ZTP, bootstrap, or service provisioning) fail, you need not delete the site. You can go to the Jobs page (**Monitor > Jobs**), select the job, and click the **Retry Job** button. If the service provisioning fails, then the site remains in the Provision-Failed state. You can review the configuration to correct any settings by editing the site.

RELATED DOCUMENTATION

[Zero Touch Provisioning Overview](#) | 259

Configure an SRX Series CPE to Discover an EX Series Switch or AP Connected to the CPE

Starting in Release 6.0.0, you can use Contrail Service Orchestration (CSO) to discover an EX Series switch that is connected to an SRX Series Customer Premise Equipment (CPE) functioning as a secure SD-WAN router or a firewall device. You can also access the Juniper Mist page to view the details of the discovered EX Series switch, or access point (AP).

The switch and the CPE can be connected through a trunk port. However, you can also use two or more trunk ports to connect the CPE and the switch and combine those ports to form a Link Aggregation Group (LAG) for higher throughput and redundancy. You can manage the switch through in-band management, where, the trunk ports carry the management traffic in addition to data.

This feature is also supported by vSRX with Junos OS Release 20.3R1 or later.

NOTE: You can configure CSO to discover a switch connected to a CPE on provisioned sites only.

To discover a switch (or AP) connected to a CPE, and view its details on Juniper Mist:

1. (Optional) Create a LAG interface if you want to use a LAG interface to connect the CPE to the switch. See [“Create LAG Interface” on page 312](#) for details.
2. Create and use a redundant Ethernet (reth) interface to connect the SRX Series CPE devices to an EX series switch (applicable only to dual CPE deployments). See [“Create a RETH Interface” on page 314](#) for details.
3. Enable LLDP on the CPE port. This step enables the CSO to discover the EX Series switch connected to the SRX Series CPE. See [“Enable LLDP on a CPE Interface” on page 311](#) for details.
4. Create management connectivity between the CPE and the switch. See [“Create Management Connectivity Between a CPE and a Switch” on page 322](#) for details.
5. Discover the EX Series switch or an access point (AP) configured behind a CPE. See [“Discover an EX Series Switch or APs Configured Behind a CPE” on page 325](#) for details.
6. Cross launch to the Juniper Mist platform to view the details of an EX Series switch, or an AP that are added in the Juniper Mist Platform. See [“View an EX Series Switch or an AP on Mist” on page 325](#) for details.

You can also view the SRX CPE details on the Juniper Mist platform (if the CPE is added to Juniper Mist). See [“View an SRX Series CPE on Juniper Mist” on page 326](#) for details.

Managing Device Images

IN THIS CHAPTER

- [Device Images Overview | 266](#)
- [About the Device Images Page | 266](#)
- [Deleting Device Images | 267](#)

Device Images Overview

An image management system provides full lifecycle management of images for all network devices, including CPE device and virtualized network function (VNF) images. A *device image* is a software installation package for the CPE device or an image for a virtual application that runs on the device. For example, for a NFX Series device platform, you require an NFX software image and a software image for the vSRX application that provides security functions and routing on the device.

RELATED DOCUMENTATION

[About the Device Images Page | 266](#)

About the Device Images Page

To access this page, click **Resources > Images**.

You can use the Images page to view the list of device images that are available in tenant's network.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a device image. Click the details icon that appears when you hover over the name of an image or click **More > Details**.

- Show or hide columns about the device image. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a device image. Click the Search icon in the top right corner of the page to search for a device image.

Field Descriptions

Table 50 on page 267 shows the fields on the Images page.

Table 50: Fields on the Device Images Page

Field	Description
Image Name	View the name of the device image. Example: juniper_srx_v1.tgz
Type	View the type of the device image. Example: VNF Image
Version	View the version number of the device image. Example: 1.1
Vendor	View the vendor name of the device. Example: Juniper
Size	View the size of the device image. Example: 14 KB

RELATED DOCUMENTATION

| [Device Images Overview](#) | 266

Deleting Device Images

You can delete one or more device images from the Device Images page.

To delete a device image:

1. Select **Resources > Images**.

The Images page appears with a list of device images.

2. Select the device image that you want to delete and then click the delete icon (X).

The Confirm Delete page appears.

3. Click **Yes** to confirm.

The Delete Success messages is displayed.

The device image is deleted.

RELATED DOCUMENTATION

| [About the Device Images Page](#) | 266

Managing Resources

IN THIS CHAPTER

- Multidepartment CPE Device Support | 270
- About the Devices Page | 271
- Perform Return Material Authorization (RMA) for a Device | 275
- Grant Return Material Authorization (RMA) for a Device | 283
- Manage a Single CPE Device | 288
- Rebooting a CPE Device | 290
- Configuring APN Settings on CPE Devices | 291
- Identifying Connectivity Issues by Using Ping | 294
- Identifying Connectivity Issues by Using Traceroute | 298
- Remotely Accessing a Device CLI | 300
- View the Current Configuration on a Device | 301
- Generate Device RSI for Enterprise Hub and Spoke Devices | 302
- Configuring the Firewall Device | 303
- About the Physical Interfaces Page | 305
- About the Logical Interfaces Page | 306
- Adding a Logical Interface | 307
- Editing, Deleting, and Deploying Logical Interfaces | 310
- Enable LLDP on a CPE Interface | 311
- Create LAG Interface | 312
- Create a RETH Interface | 314
- Create a Redundancy Group | 316
- Manage Redundancy Groups | 317
- Adding a Security Zone | 318
- Adding a Routing Instance | 321
- Create Management Connectivity Between a CPE and a Switch | 322
- Discover an EX Series Switch or APs Configured Behind a CPE | 325
- View an EX Series Switch or an AP on Mist | 325
- View an SRX Series CPE on Juniper Mist | 326

- [About the Static Routes Page | 326](#)
- [Adding a Static Route | 327](#)
- [Editing, Deleting, and Deploying Static Routes | 330](#)

Multidepartment CPE Device Support

Support for multiple departments in a CPE device enables sites (branch, cloud spoke, and enterprise hubs) to be mapped to serve across multiple departments within a single tenant. An overlay tunnel [generic routing encapsulation (GRE) or GRE over IPsec] is used to carry traffic from all departments in a site, to another site, an enterprise hub or a provider hub,) by separating the traffic for each department through MPLS-based traffic separation.

Support for multiple departments in a single CPE device is a cost-effective approach where the cost of a device and its maintenance is shared among multiple departments in a tenant.

For more information about departments, see [“About the Departments Page” on page 781](#).

A tenant administrator can perform the following tasks related to departments:

- View all departments configured on an activated CPE device.
- Manage and monitor all policies and dashboards for all departments in a site.
- Create SD-WAN and security policies and monitor the dashboard at the site level or at the department level.

Add traffic-based steering profiles and map them to SD-WAN policies for traffic management.

- View the shared CPE device and its services and networks even though the WAN links might be shared by multiple departments.

Overlapping IP Addresses Across Departments

Starting from CSO Release 5.4.0, you can use same IP addresses across multiple departments in a network segmentation-enabled tenant. When network segmentation is enabled for a tenant, each department has its own VRFs. This allows overlapping IP addresses to be used across different departments.

When network segmentation is not enabled for a tenant, all departments in the tenant use the same VRFs. Therefore, the IP addresses used across the departments should be unique.

The following are some scenarios for using overlapping IP addresses across departments in a tenant:

- The HR department in site Chicago and the Sales department in site Boston can have overlapping IP addresses.
- The HR department and Sales department in site Chicago can have overlapping IP addresses.

The HR department when used in both Chicago and Boston sites cannot have overlapping IP addresses as the same VRFs are used by both the sites. In this case, the IP addresses used by the HR department in Chicago should be different from IP addresses used by the HR department in Boston.

When you use overlapping IP addresses across departments, you must configure an IP pool-based source NAT rule for Zscaler breakout.

- When traffic from a site (spoke or enterprise hub) is breaking out to Zscaler at the site, the NAT rule should have the source as the department zones that have overlapping IP addresses and destination as untrust zone. This NAT rule should be deployed at the site where the traffic is originating.
- When traffic from a spoke site is breaking out to the Zscaler tunnel at an enterprise hub site, the NAT rule should have source as trust zone and the destination as untrust zone. This NAT rule should be deployed at the enterprise hub.

For information about creating NAT rules, see [“Creating NAT Policy Rules” on page 638](#).

NOTE:

- Firewall policy intents will use VRF groups of a department in intent rules for allowing site-to-site traffic.
- NAT rules created automatically for Internet traffic from spoke to enterprise hub (flowing from overlay to underlay) will use VRF groups to egress interface instead of trust zone.

RELATED DOCUMENTATION

[About the SLA Performance of a Single Tenant Page | 856](#)

[Viewing the SLA Performance of a Site | 859](#)

About the Devices Page

To access this page, click **Resources > Devices**.

You can use the Devices page to view the list of all devices managed by Contrail Service Orchestration (CSO). You can also view information about each device in the network.

Tasks You Can Perform

You can perform the following tasks from this page:

- Manage a CPE. See [“Manage a Single CPE Device” on page 288](#).
- Reboot a CPE device. See [“Rebooting a CPE Device” on page 290](#).
- Download the cloud formation template. Click **Cloud Info Template** to download the template in JSON format. See [“Download the Cloud Formation Template” on page 117](#) and [“Provision the Device on AWS Server” on page 117](#).
- Activate a device. See [“Activate a Device” on page 252](#). You can also view detailed information about the device activation logs at **More > Activation Logs**. See [“Viewing the History of Tenant Device Activation Logs” on page 257](#).
- Push licenses to devices. Select the device and click **Push License**. See *Pushing a License to Devices*.
- View stage-1 configuration. Click **Stage-1 Config** and copy or save the configuration and deploy it to a device. See [“Workflow for Onboarding a Device Using ZTP” on page 262](#).
- Perform Return Material Authorization (RMA) to replace a device that is faulty or not reachable. You can perform RMA for a single-CPE, dual-CPE, provider hub, enterprise hub, and next-generation firewall devices.
 - For information on performing RMA on single-CPE, dual-CPE, enterprise hub, and next-generation firewall devices, see [“Perform Return Material Authorization \(RMA\) for a Device” on page 275](#)
- View details about a device. Click the Detail icon that appears when you hover over the row for a device or select a device and click **More > Detail**.
- Install certificates on the site. See [“Installing and Uninstalling Certificates” on page 421](#).
- Ping a remote host from a device to identify connectivity issues. See [“Identifying Connectivity Issues by Using Ping” on page 294](#).
- Access the CLI of a device remotely. See [“Remotely Accessing a Device CLI” on page 300](#).
- Traceroute a remote host from a device to identify connectivity issues. See [“Identifying Connectivity Issues by Using Traceroute” on page 298](#).
- Show or hide columns about a device. Click the **Show/Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Filter and sort the devices. Click a column name to sort the devices based on the column name.
Click the filter icon and select whether you want to show or hide column filters or apply a quick filter.

NOTE: Sorting and filtering is applicable only to some fields.

- Search for a device. Click the Search icon in the top right corner of the page to search for a specific device.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

Table 51 on page 273 describes the fields on the Devices page.

Table 51: Fields on the Devices Page

Field	Description
Device Name	Displays the name of the device. Example: sunny-NFX-250
Tenant	Displays the name of the tenant. Example: tenant-blue
Site Name	Displays the name of the tenant site. Example: site-blue-white

Table 51: Fields on the Devices Page *(continued)*

Field	Description
Management Status	<p>Displays the management status of the CPE devices deployed in the cloud.</p> <ul style="list-style-type: none"> • EXPECTED—Regional server has the activation details for the CPE device, but CPE device has not yet established a connection with the server. • DEVICE DETECTED—Device is configured and is reachable by CSO. After the user enters the activation code for the device, the activation code is validated and device is authenticated. • RMA—CPE device has been tagged for RMA as a result of the user applying the Initiate RMA action on the device. • ACTIVE—ZTP is initiated, CPE device has downloaded images, but not yet configured, and stage-1 configuration is pushed to the device. • PROVISIONED—ZTP is complete, and IPsec tunnel is established and operational on the device. • PROVISION_FAILED—Multiple factors lead to failure in provisioning a device. If any of the steps in ZTP fails or if any process fails as a part of device activation, then provision fails. For example, CPE device provisioning fails when the vSRX is not instantiated properly.
Model	<p>Displays the name of the device model.</p> <p>Example: NFX</p>
Active Services	<p>Displays the number of services that are activated for the device.</p> <p>Example: 3</p>
Operational Status	<p>Displays whether the device is up or down.</p>
Location	<p>Displays the name of the location.</p> <p>Example: San Jose, CA</p>
Status Message	<p>Displays the latest status message.</p> <p>Example: IPsec provision success</p>
WAN Links	<p>Displays the number of WAN links.</p> <p>Example: 2</p>
POP Name	<p>Displays the name of the POP.</p> <p>Example: pop_blue</p>

Table 51: Fields on the Devices Page *(continued)*

Field	Description
Image Name	Displays the name of the device image file. Example: install_nfx_fmfm_agent_1_0.sh
OS Version	Displays the Junos OS Release version. Example: 15.1X49-D40
Serial Number	Displays the serial number of the device. Example: XXXXXXXXXXXXX
UUID	Displays the universally unique identifier (UUID) of the device. Example: xxxxxxxx-xxxx-xxxx-xxx-xxxxxxxxxxxx

RELATED DOCUMENTATION

[Manage a Single CPE Device](#) | 288

Perform Return Material Authorization (RMA) for a Device

IN THIS SECTION

- [Perform Return Material Authorization \(RMA\) for a Single-CPE, Enterprise Hub and Next-Generation Firewall](#) | 276
- [Perform Return Material Authorization \(RMA\) for a Dual-CPE Device](#) | 278

Sometimes, due to hardware failure, a device managed by Contrail Service Orchestration (CSO) needs to be returned to the vendor for repair or replacement. In such situations, you, as the tenant administrator, can perform Return Material Authorization (RMA) for the faulty device.

From Customer Portal, you can perform RMA for single-CPE, dual-CPE, enterprise hub, and Next-Generation Firewall devices.

The RMA process includes actions to:

1. Back up the configuration of the faulty device.
2. Recall the faulty device and replace it with a new or restored device.
3. Push the required configuration to the new or restored device.
4. Activate the new or restored device in order for CSO to recognize and manage the device.

Perform Return Material Authorization (RMA) for a Single-CPE, Enterprise Hub and Next-Generation Firewall

When you request RMA for a non-SRX device (NFX single-CPE device) associated with a site that has a version earlier than the CSO version, the site version is upgraded to the CSO version. The site version is upgraded as part of the device activation and zero touch provisioning (ZTP) process of the replacement device that is performed after RMA.

When you request RMA for an SRX single-CPE device, enterprise hub device, or next-generation firewall device associated with a site that has a version earlier than the CSO version, the site version is not upgraded to the CSO version as part of the device activation and zero touch provisioning (ZTP) process of the replacement device that is performed after RMA.

To perform RMA for a single-CPE, enterprise hub, next-generation firewall:

1. Select **Resources > Devices**.

The **Devices** page appears.

2. Select the faulty device and click **More > Initiate RMA**.

A confirmation page appears requesting for confirmation to initiate the RMA process for the device.

NOTE:

- The **Initiate RMA** option is enabled only for a device with the management status **PROVISIONED**.

3. Click **Yes** to confirm RMA for the device.

You are returned to the Devices page where a confirmation message appears, indicating that the RMA process is initiated.

4. After the management status of the device changes to **RMA**, raise a device replacement request. This action is performed outside of CSO.

5. After you receive the new device, click **More > Grant RMA**.

The Grant RMA for Device page appears. Provide details of the new device on this page. See [“Grant Return Material Authorization \(RMA\) for a Device” on page 283](#) for details.

NOTE:

- The **Grant RMA** option is enabled only for a device with the management status **RMA**.
- Before you grant RMA, ensure that you have uploaded the required license for the new device.

6. To complete the RMA process and start using the new device, the device must be activated.

- If you enabled the Auto-activate toggle button on the Grant RMA for Device page, the device is activated automatically and its **Management Status** changes to **PROVISIONED**.
- If you disabled the Auto-activate toggle button on the Grant RMA for Device page, you must activate the new device manually after the grant RMA job completes successfully.

To activate the new device manually:

- a. On the Devices page, select the new device and click **Activate Device**.

The Activate Device page appears.

- b. Enter the activation code for the device and click **Next**.

The progress of device activation is displayed.

After the device is activated, its **Management Status** changes to **PROVISIONED**.

7. • If the device for which you performed RMA is an SRX Series single-CPE device, enterprise hub device, or next-generation firewall device, the RMA process is now complete. You can start using the new device.
- If the device for which you performed RMA is an NFX150 or NFX250 device, an **RMA** tag is also displayed beside the management status indicating that the RMA process is not yet complete. Hover over the RMA tag to see the additional steps that you need to perform to complete the RMA process.

Push the following configuration to the newly provisioned device manually:

- Licenses—Generate a new license and upload it to CSO. See [“About the Device Licenses Page” on page 401](#).
- Application Signatures—Push the application signatures to the new device. See [“About the Application Signatures Page” on page 769](#).

- Certificates—Import and install the required certificates on the new device. See [“Importing a Certificate” on page 419](#) and [“Installing and Uninstalling Certificates” on page 421](#).
- Policies—Push the defined firewall and NAT policies to the new device. See [“About the Firewall Policy Name Page” on page 444](#) and [“About the NAT Policies Page” on page 632](#).

To complete the RMA process, you must remove the RMA tag manually. To remove the RMA tag, hover over the **PROVISIONED (RMA)** tag, select the check box indicating that you have completed all the steps for RMA, and click **OK**.

The RMA process is now complete. You can start using the new device.

Perform Return Material Authorization (RMA) for a Dual-CPE Device

IN THIS SECTION

- [Perform RMA for an NFX Cluster | 278](#)
- [Perform RMA for an SRX Cluster | 281](#)

You can perform RMA for devices in an NFX or SRX cluster when the devices fail or need to be replaced with new devices.

Perform RMA for an NFX Cluster

From CSO Release 4.1.0 onward, when an NFX250 device in a dual CPE cluster fails, you can perform RMA for only the failed device. In releases before CSO Release 4.1.0, RMA must be performed for both the devices in the cluster.

To perform RMA for an NFX cluster:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

- a. Select **Resources > Site Management**.

The Sites page appears.

- b. Click a site that contains the NFX cluster for which you want to perform RMA.

The *Site-Name* page appears.

- c. Click the **Devices** tab to view the devices and clusters installed at the site.

NOTE: On a site associated with an NFX dual-CPE device, if the site version is earlier than that of the CSO version, you can perform RMA only at the cluster level. After RMA of the cluster, the version of the site is upgraded to that of CSO as part of the device activation and ZTP process of the replacement devices in the cluster.

2. Do one of the following:

- To perform RMA at the cluster level, select the cluster and click **More > Initiate RMA**.
- To perform RMA for a single device in the cluster, select the device and click **More > Initiate RMA**.

A confirmation page appears requesting for confirmation to initiate the RMA process.

3. Click **Yes** to confirm RMA for the selected NFX cluster or device.

You are returned to the Devices page where a confirmation message appears indicating that the RMA process is initiated for the selected NFX cluster or device.

NOTE:

- The **Initiate RMA** option is enabled only for an NFX cluster or device with the management status **PROVISIONED**.
- On the Sites page (**Resources > Site Management**), the status of the site, where the NFX cluster or the device for which you initiated RMA is installed, remains as **PROVISIONED**. However, a red-colored **RMA** tag appears beside the **Site Status** to indicate that RMA is initiated for a cluster or device at the site.

4. After the NFX cluster or device is in the **RMA** state, you can raise a device replacement request for one or more faulty devices in the NFX cluster. This action is performed outside of CSO.

5. After you receive the new device or devices, click **More > Grant RMA**.

The Grant RMA for Device page appears. Provide details of the new device or devices. See [“Grant Return Material Authorization \(RMA\) for a Device” on page 283](#) for details.

NOTE:

- The **Grant RMA** option is enabled only for a device with the management status **RMA**.
- Before you grant RMA, ensure that you have uploaded the required license for the new device.

6. To complete the RMA process and start using the new device or devices, the device or devices must be activated.
 - If you enabled the Auto-activate toggle button on the Grant RMA for Device page, the device or devices are activated automatically and the **Management Status** changes to **PROVISIONED**.
 - If you disabled the Auto-activate toggle button on the Grant RMA for Device page, you must activate the new device or devices manually.

To activate the device or devices in the NFX cluster manually:

- a. On the Devices page, do one of the following:
 - To activate both the devices in the cluster, select the cluster (if the entire cluster is RMAed) and click **Activate Device**.
 - To activate a single device in the cluster, select the device (if a single device is RMAed) and click **Activate Device**.

The Activate Device page appears.

- b. Enter the activation code for the device and click **Next**.

The progress of device activation is displayed.

After the device is activated, its **Management Status** changes to **PROVISIONED**.

An RMA tag is displayed beside the management status indicating that the RMA process is not yet complete. Hover over the RMA tag to see the additional steps that you need to perform to complete the RMA process.

7. Push the following configuration to the newly provisioned devices manually:

NOTE:

- In SD-WAN deployments, once the new devices are in the **PROVISIONED** state, you can proceed to configure the devices by pushing application signatures, certificates, and policies manually.
 - When you perform RMA on a single device, CSO restores certificates on the new device. However, application signatures and policies need to be pushed manually.
- Application Signatures—Push the application signatures to the replaced device. See [“About the Application Signatures Page” on page 769](#).
 - Certificates—Import and install the required certificates on the replaced devices. See [“Importing a Certificate” on page 419](#) and [“Installing and Uninstalling Certificates” on page 421](#).

- Policies—Push the defined firewall and NAT policies to the replaced devices. See [“About the Firewall Policy Name Page” on page 444](#) and [“About the NAT Policies Page” on page 632](#).
8. To complete the RMA process, you must remove the RMA tag manually. To remove the RMA tag, hover over the **PROVISIONED (RMA)** tag, select the check box indicating that you have completed all the steps for RMA, and click **OK**.

The RMA process is now complete. You can start using the new device.

Perform RMA for an SRX Cluster

For an SRX cluster, you can perform RMA on a member device of the cluster. That is, you can select the faulty device from the SRX cluster and perform RMA on it individually. You cannot perform RMA for an SRX cluster at the cluster level.

To return a faulty device in an SRX cluster and replace it with a new or restored device by using RMA:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

- a. Select **Resources > Site Management**.

The Sites page appears.

- b. Click a site that contains the SRX cluster for which you want to perform RMA.

The *Site-Name* page appears.

- c. Click the **Devices** tab to view the devices and clusters installed at the site.

2. Select the faulty device in the SRX cluster and click **More > Initiate RMA**.

A confirmation page appears requesting for confirmation to initiate the RMA process for the device.

3. Click **Yes** to confirm RMA for the device.

You are returned to the Devices page where a confirmation message appears, indicating that the RMA process is initiated.

NOTE:

- The **Initiate RMA** option is enabled only for a device with the management status **PROVISIONED**.
- On the Sites page (**Resources > Site Management**), the status of the site, where the device for which you initiated RMA is installed, remains **PROVISIONED**. However, a red-colored **RMA** tag appears beside the current site status to indicate that RMA is initiated for a cluster or device at the site.

4. After the management status of the device changes to RMA, you must raise a replacement request for the faulty device in the SRX cluster. This process is performed outside of CSO.
5. After you receive the new device, click **More > Grant RMA** to provide details of the new device. See [“Grant Return Material Authorization \(RMA\) for a Device” on page 283](#) for details.

NOTE:

- The **Grant RMA** option is enabled only for a device with the management status **RMA**.
- Before you grant RMA, ensure that you have uploaded the required license for the new device from the Device Licenses page (**Administration > License > Device Licenses**).

6. To complete the RMA process, you must remove the RMA tag manually. To remove the RMA tag, hover over the **PROVISIONED (RMA)** tag, select the check box indicating that you have completed all the steps for RMA, and click **OK**.

The RMA process is now complete. You can start using the new device.

RELATED DOCUMENTATION

[About the Devices Page | 271](#)

[Grant Return Material Authorization \(RMA\) for a Device | 283](#)

Grant Return Material Authorization (RMA) for a Device

IN THIS SECTION

- [Grant Return Material Authorization \(RMA\) for a Single-CPE, Enterprise Hub, and Next-Generation Firewall | 283](#)
- [Grant RMA for a Dual-CPE Device | 285](#)
- [Grant RMA for an SRX Device within an SRX Cluster | 287](#)

As a Tenant Administrator with the RMA privilege, you can grant RMA for a single CPE, dual CPE, enterprise hub, and next-generation firewall devices from the Customer Portal. When you grant RMA, the device-related configuration is backed up to the CSO database, the existing device is recalled, and the new device is added to the network.

Before you grant RMA for a device, ensure that:

- You have received a new device for replacing the faulty device.
- You have the serial number and activation code for the new device.
- You have uploaded the required license for the new device.

Grant Return Material Authorization (RMA) for a Single-CPE, Enterprise Hub, and Next-Generation Firewall

To grant RMA for a single CPE, enterprise hub, or next-generation firewall:

1. Select **Resources > Devices**.

The **Devices** page appears.

Alternatively,

- a. Select **Resources > Site Management**.

The **Sites** page appears.

- b. Click a site that contains the device for which you want to perform RMA.

The **Site-Name** page appears.

c. Click the **Devices** tab to view the devices and clusters installed at the site.

2. Select the faulty device for which you initiated RMA and click **More > Grant RMA**.

The Grant RMA for Device page appears.

NOTE: The **Grant RMA** option is enabled only for devices with the management status **RMA**.

3. Complete the configuration according to the guidelines provided in [Table 52 on page 284](#).

4. Click **OK** to perform the grant RMA process.

You are returned to the Devices page where a confirmation message appears indicating that a Grant RMA job is created.

5. (Optional) Click the job link in the message to view the progress of the job. Alternatively, view the progress of this job on the Jobs (**Monitor > Jobs**) page. This job might take around 15 minutes to complete.

After the job completes successfully, the management status of the device on the Devices page changes to **Expected**. In addition, the status of the site on the Sites page (**Resources > Site Management**), where the device for which you performed Grant RMA is installed, changes to **Expected**.

To complete the RMA process and start using the new device, you must activate the device. See step 6 in [“Perform Return Material Authorization \(RMA\) for a Device” on page 275](#) for details.

[Table 52 on page 284](#) provides guidelines on using the fields on the Grant RMA for Device page.

Table 52: Fields on the Grant RMA for Device Page

Field	Description
Customer Name	Displays the name of the tenant who is performing RMA.
Site Name	Displays the name of site in which the faulty device is present.
Device Name	Displays the name of the faulty device that will be replaced with a new device through the Grant RMA process.
Auto Activate	Click the toggle button to enable (default) or disable automatic activation of the new device.

Table 52: Fields on the Grant RMA for Device Page (*continued*)

Field	Description
Activation Code	If you disable automatic activation, enter the activation code for the new device. You receive the activation code (Example: 545454) from the service provider, outside of CSO.
Serial Number	Enter the serial number of the new device. The serial number is case-sensitive. Example: DD2316AF0177
Boot Image	<p>Select the boot image from the list if you want to upgrade the image for the device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when CSO starts the ZTP process.</p> <p>NOTE: For SRX devices, select the same boot image as the faulty device. If you select a different boot image for the new device, the grant RMA process may not complete successfully.</p>

Grant RMA for a Dual-CPE Device

To grant RMA for a dual-CPE device (cluster):

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

a. Select **Resources > Site Management**.

The Sites page appears.

b. Click a site that contains the dual-CPE device for which you initiated RMA.

The *Site-Name* page appears

c. Click the **Devices** tab to view the devices and clusters installed at the site.

2. Select the cluster or the device in the cluster for which you initiated RMA and click **More > Grant RMA**.

The **Grant RMA for Device** page appears.

NOTE: The **Grant RMA** option is enabled only for devices with the Management Status **RMA**.

3. Complete the configuration according to the guidelines provided in [Table 53 on page 286](#).

4. Click **OK** to perform the grant RMA process.

You are returned to the Devices page where a confirmation message appears indicating that a Grant RMA job is created.

When you grant RMA, the following actions are performed:

- The cluster-related configuration is backed-up to the CSO database, and the devices in the cluster are recalled and the new or restored devices are added to the network.
- The management status of the cluster changes to **EXPECTED** on the **Devices** page. An **RMA** tag is also displayed beside the management status indicating that the RMA process is not yet complete. Hover over the RMA tag to see the additional steps that you must perform to complete the RMA process.

On the Sites page (**Resources > Site Management**), the status of the site, where the cluster or device for which you performed **Grant RMA** is installed, changes to **Expected**.

5. (Optional) View the progress of this job on the Jobs (**Monitor > Jobs**) page. This job might take around 15 minutes to complete.

[Table 53 on page 286](#) provides guidelines on using the fields on the **Grant RMA for Device** page.

Table 53: Fields on the Grant RMA for Dual-CPE Device Page

Field	Description
Customer Name	Displays the name of the tenant performing RMA.
Site Name	Displays the name of site in which the faulty device is present.
Device Name	Displays the name of the faulty device that will be replaced with new or restored devices through the Grant RMA process.
Primary Serial Number	Enter the serial number of the new primary device. The serial number is case-sensitive. Example: DD2316AF0177
Primary Activation Code	Enter the activation code for the new primary device. You will receive the activation code from the service provider, outside of CSO. Example: 545454
Secondary Serial Number	Enter the serial number of the new secondary device. The serial number is case-sensitive. Example: DD2316AF0145
Secondary Activation Code	Enter the activation code for the new secondary device. You receive the activation code from your service provider, outside of CSO. Example: 545476

Grant RMA for an SRX Device within an SRX Cluster

To grant RMA for an SRX Series device within an SRX cluster:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

- a. Select **Resources > Site Management**.

The Sites page appears.

- b. Click the site that contains the SRX device for which you initiated RMA.

The *Site-Name* page appears

- c. Click the **Devices** tab to view the devices and clusters installed at the site.

2. Select the defective device for which you initiated RMA and click **More > Grant RMA**.

The **Grant RMA for Device** page appears.

NOTE: The **Grant RMA** option is enabled only for devices with the Management Status **RMA**.

3. Complete the configuration according to the guidelines provided in [Table 54 on page 288](#).

4. Click **OK** to perform the grant RMA process.

You are returned to the Devices page where a confirmation message appears indicating that a Grant RMA job is created.

When you perform Grant RMA for a device, a job is created to update the device object in CSO with the serial number and activation code of the new device. On the Sites page (**Resources > Site Management**), the status of the site, where the device for which you performed Grant RMA is installed, changes to **PROVISIONED**.

5. View the progress of this job on the Jobs (**Monitor > Jobs**) page. This job might take around 15 minutes to complete.

[Table 54 on page 288](#) provides guidelines on using the fields on the **Grant RMA for Device** page.

Table 54: Fields on the Grant RMA for Device Page (for SRX Device in an SRX Cluster)

Field	Description
Customer Name	Displays the name of the tenant who is performing RMA.
Site Name	Displays the name of site in which the faulty device is present.
Device Name	Displays the name of the faulty device that will be replaced with a new one through the Grant RMA process.
Serial Number	Enter the serial number of the new device. The serial number is case-sensitive. Example: DD2316AF0177
Activation Code	Enter the activation code for the new device. You receive the activation code (Example: 545454) from the service provider, outside of CSO.

RELATED DOCUMENTATION

[About the Devices Page | 271](#)

[Perform Return Material Authorization \(RMA\) for a Device | 275](#)

Manage a Single CPE Device

Users with the Tenant Administrator role can use the **Device-Name** page (**Resources > Devices > Device-Name**) to view details of and manage a customer premises equipment (CPE) device.

This topic provides information about managing a CPE device.

To manage a CPE device:

- Click the **Overview** tab to perform the following operations:
 - View the geographical location of the device at the tenant site.
 - View the aggregate throughput of the device.
 - View recent alerts for the device.
 - View recent alarms for the device.

- View license details of the device.
- View details of the device, such as serial number, management IP address, OS version, device template, tenant name, site name, operational status, and management status.
- Click the **Inventory** tab to perform the following operations:
 - Click the **Chassis** tab to view the hardware details
 - Click the **Physical Interfaces** tab to view the physical interfaces for the device.
 - Click the **Logical Interfaces** tab to view the logical interfaces for the device.
 - Click the **Licenses** tab to view and manage the device and feature licenses on the device.
 - Click the **Software** tab to view and manage the software images on the device.
- Click the **Configuration Template** tab to perform the following operations:
 - Click + to add a new template.
 - Select a template and click **Configure** to edit an existing template. In the Configure page, you can:
 - Click **View Changes** to view the changes between the current and previous configuration.
 - Click **Render Template** to render a configuration in CLI format.
 - Click **Deploy** to deploy a configuration.
 - Click **Undeploy** to undeploy a configuration template from a device.
Undeploying a configuration template removes the configuration pushed to the device when the configuration template was deployed.
 - Click **Dissociate** to dissociate a configuration template from a device.
Dissociating a configuration template removes only the references to the configuration template from the device but does not remove the configuration pushed to the device.
 - Click **Deployment History** to view the deployment history.
- Click the **Configuration** tab to perform the following operations (applicable only for Next-Generation Firewall devices):
 - Click the **Interfaces** tab to add the LAG interfaces (for a single SRX device) or RETH interfaces (for dual SRX devices) to manage the connectivity between the device and a switch.
 - Click the **Zones** tab to view and manage the security zones for the device.
 - Click the **Redundancy Group** tab to add or edit redundancy group information. This tab is displayed only for dual SRX devices connected as a cluster.
 - Click the **Running Configuration** tab to view the current configuration on the device. Click the **Remote Console** option to access the device CLI. You can automatically log in to the device through the Remote

Terminal browser window, without entering a username and password. If you access the device CLI through the remote terminal, root user login is disabled.

RELATED DOCUMENTATION

| [About the Devices Page](#) | 271

Rebooting a CPE Device

You need to reboot a CPE device if the device is down, or if all troubleshooting options fail.

To reboot a CPE device:

1. Select **Resources > Devices**.
2. Select the CPE device that you want to reboot and select **More > Reboot**.

A Device Reboot job link is created and the Status Message column displays the status as **Reboot in-progress**.

NOTE: If you reboot a tenant device, deployments that are in progress are stopped.

3. (Optional) Click the **Device Reboot** link to view the device reboot logs.
4. (Optional) You can view the job status on the **Monitor > Jobs** page.

You can view the status of reboot in the Status Message column.

On successful reboot of the CPE device, the Status Message column displays the status as **Reboot Succeeded**.

If a CPE device is not reachable or if the reboot time exceeds the timeout value, the reboot fails and the Status Message column displays the status as **Reboot Failed**.

NOTE: The timeout value for rebooting a CPE device is 14 minutes.

RELATED DOCUMENTATION

[About the Devices Page | 271](#)

Configuring APN Settings on CPE Devices

IN THIS SECTION

- [Configuring APN Settings with SIM Change on CPE Devices | 291](#)
- [Configuring APN Settings without SIM Change on CPE Devices | 293](#)

You can configure Access Point Name (APN) settings on the following devices, with or without SIM change. You can change the APN settings either to use a private APN with the current LTE service provider or to use a different LTE service provider.

NOTE: You can only insert a SIM card in the SIM1 slot of the LTE Mini-Physical Interface Module (Mini-PIM).

Following is the list of devices on which you can configure APN settings:

- NFX Series—NFX150 and NFX250 CPE devices
- SRX Series—SRX320, SRX340, and SRX345 CPE devices

Configuring APN Settings with SIM Change on CPE Devices

To configure APN settings with SIM change:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device that you want to configure.

The *Device-Name* page appears.

3. Click the **Configuration Template** tab and change the APN settings according to the guidelines provided in [Table 55 on page 292](#).

4. Click **Save**.

The new settings are applied after one minute.

5. Remove the USB dongle from the CPE device, change the SIM card, and re-insert the USB dongle.

The system checks for the new APN settings every minute.

- If the applied APN settings are compatible with the new SIM card—The LTE WAN link and its tunnels go down after one minute and remain down till the new SIM card is inserted. The LTE dongle LED indicates that the connection is down during this period. Maximum one minute after the new SIM is inserted, the LTE dongle LED indicates that the connection is up. The LTE WAN link and its tunnels come up automatically.
- If the applied APN settings are not compatible with the new SIM card—The LTE WAN link and its tunnels go down after one minute and remain down even after the new SIM card is inserted. The LTE dongle LED indicates that the connection is down even after the new SIM is inserted.

6. To revert to the old SIM, remove the USB dongle, replace the current SIM with the previous SIM, and re-insert the dongle.

The system checks for the new APN settings every minute. Maximum one minute after the old SIM is inserted, the LTE dongle LED indicates that the connection is up (using the old SIM and old APN). The LTE WAN link and its tunnels come up automatically.

Table 55: Fields for the APN Configuration Settings on the Configuration Template Tab

Field	Description
Edit Settings for APN Configuration	
Use default APN settings	<p>Click the toggle button to enable (default) or disable the default APN settings.</p> <ul style="list-style-type: none"> • If you enable this option, the default APN settings that are shipped along with the CPE device are used for configuring the APN. • If you disable this option, you must configure the APN settings manually.
APN Settings	
APN Name	Enter the access point name (APN) of the gateway router.
SIM Change Required	<p>Click the toggle button to enable or disable changing the SIM card:</p> <p>NOTE: You can change the SIM card either to use a different LTE service provider or to use a private APN with the current LTE service provider.</p> <ul style="list-style-type: none"> • (Default) Enable this option to change the APN settings and to use a new SIM card. • Disable this option to change the APN settings without changing the SIM card.

Table 55: Fields for the APN Configuration Settings on the Configuration Template Tab (*continued*)

Field	Description
Authentication Method	<p>From the list, select one of the following authentication methods for the APN configuration as configured by the service provider:</p> <ul style="list-style-type: none"> • (Default) PAP—Select this option to use Password Authentication Protocol (PAP) as the authentication method. • CHAP—Select this option to use Challenge Handshake Authentication Protocol (CHAP) authentication as the authentication method. • None—Select this option if you do not want to use any authentication method.
Authentication Information	
SIP User ID	Enter the Session Initiation Protocol (SIP) user ID for authentication.
SIP Password	Enter the SIP password for authentication.

Configuring APN Settings without SIM Change on CPE Devices

To configure APN settings without SIM change:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device that you want to configure.

The *Device-Name* page appears.

3. Click the **Configuration Template** tab and change the APN settings according to the guidelines provided in [Table 55 on page 292](#).

4. Click **Save**.

The new settings will be applied after one minute.

- If the applied APN settings are valid—In CSO, the LTE WAN link and its associated tunnels go down momentarily and then, get re-established automatically.
- If the applied APN settings are invalid—After one minute, the LTE dongle LED indicates that the connection is down. In CSO, the LTE WAN link and its associated tunnels go down.

After two minutes, the LTE dongle LED indicates that the connection is up (using old APN). In CSO, the LTE WAN link and its tunnels come up automatically.

RELATED DOCUMENTATION

[About the Devices Page](#) | 271

Identifying Connectivity Issues by Using Ping

You can use Contrail Service Orchestration (CSO) to perform a ping operation from a device (provider hub, tenant device, CPE device, enterprise hubs, or next-generation firewall device) to a remote host for identifying issues in connectivity with the remote host.

When you ping a remote host from a device, an Internet Control Message Protocol (ICMP) packet is sent to the remote host. By analyzing the results of the ping operation, you can identify the possible device connectivity issues between the remote host and the device.

NOTE: In Contrail Service Orchestration (CSO) Release 6.1.0, the following devices support ping:

- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600
- vSRX

To perform the ping operation:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select a device from the list of devices displayed and click **More > Ping**.

The Ping page appears.

NOTE: You can ping from a device only when its operational status is Up in CSO.

3. Complete the configuration according to the guidelines provided in [Table 56 on page 295](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **Ping** to initiate the ping request.

A job is created and the Ping Progress page appears. After the device sends the ping packets, the Ping Result page appears. . If the ping operation is successful, the Ping Result page displays the parameters specified in [Table 57 on page 297](#).

If the ping operation fails, the Ping Result page displays an appropriate error message (such as **No response** or **No route to host**), indicating that there is an issue in the connectivity to the remote host.

Table 56: Fields on the Ping page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.
Ping Request Packets	Enter the number of ping request packets to be sent to the remote host. Default: 5. Range: 1 through 300.
Advanced	
Source Interface	Select the source interface on the device through which you want to send the ping request to the remote host. If you do not select a source interface, ping requests are sent on all interfaces. To clear the selected interface, click Clear All and select another interface.
Hostname Resolution	Click the toggle button to enable or disable (default) the display of hostname of the hops along the path to the remote host.

Table 56: Fields on the Ping page (*continued*)

Field	Description
Rapid Ping	<p>Click the toggle button to enable or disable (default) sending ping requests rapidly.</p> <p>If you enable this option, the source device sends a minimum of 100 ping request packets per second or sends a packet as soon as a response to the previous packet is received, whichever is greater.</p> <ul style="list-style-type: none"> • If the source device does not receive a response for 500 ms, timeout is considered. • If the source device receives a response within 500 ms, the next ping request packet is sent immediately. <p>NOTE: The ping results are displayed in a single consolidated message instead of individual messages for each ping request packet sent.</p>
Packet Fragmentation	<p>Click the toggle button to enable or disable (default) the fragmenting of ping request packets.</p> <p>If packet fragmentation is disabled, ping packets with the maximum transmission unit (MTU) greater than 1500 bytes are dropped.</p>
Packet Size (bytes)	<p>Enter the size (in bytes) of the ping request packet.</p> <p>Default: 56 bytes.</p> <p>Range:</p> <ul style="list-style-type: none"> • 1 through 1,472 bytes, if packet fragmentation is disabled. • 1 through 65,468 bytes, if packet fragmentation is enabled.
Wait Time (seconds)	<p>Enter the time (in seconds) for which the source device waits for a response to the ping request packet. The source device considers the remote host as not reachable after the wait time elapses.</p> <p>Default: 10 seconds.</p> <p>Range: 0 through 600 seconds.</p>
Incoming Interface	<p>Click the toggle button to include or exclude (default) information (on the Ping Result page) about the interface on the source device that receives the ping responses..</p>

Table 56: Fields on the Ping page (*continued*)

Field	Description
Routing Instance	<p>Select a specific routing instance that the ping request packets can use to reach the remote host.</p> <p>The ping result displays the information about the connectivity between the source device and the remote host based on the selected routing instance.</p> <p>To clear the selected routing instance, click Clear All and select another routing instance.</p>

Table 57: Fields on the Ping Result page

Field	Description
Packet Loss	Displays the percentage of ping packets sent for which the source device did not receive a response.
Round Trip Time Taken (in μ s)	<p>Displays the following information about the duration (in microseconds) between the time when the source device sends the ping request and the time when the source device receives a response from the remote host.</p> <p>Displays the following:</p> <ul style="list-style-type: none"> • Minimum: The minimum time taken to receive a response for a ping request packet. • Maximum: The maximum time taken to receive a response for a ping request packet. • Average: The average time taken to receive a response for all the ping request packets sent in a ping operation. • Standard Deviation: The variation of the round trip time from the mean round trip time.

Details

Sequence	Sequence number of all the ping request packets.
Result	Result of the ping request packets—Success or Failure.
Incoming Interface	<p>Interface on the source device on which the responses are received for the ping requests.</p> <p>This data appears if you have enabled the Incoming Interface option on the Ping page.</p>
Time Taken	Time taken (in microseconds) to receive response to a ping request packet.

Identifying Connectivity Issues by Using Traceroute

You can use Contrail Service Orchestration (CSO) to perform a traceroute operation from a device (provider hub, tenant device, CPE device, enterprise hubs, or next-generation firewall device) to the remote host. Traceroute helps you view the path that a packet travels to reach the remote host. The result is useful in identifying the point of network failure in the path between the source device and remote host.

NOTE: In Contrail Service Orchestration (CSO) Release 6.1.0, the following devices support traceroute:

- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600
- vSRX

To perform traceroute operation:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select a device from the list of devices displayed and Click **More > Traceroute**.

The Traceroute page appears.

3. Complete the configuration according to the guidelines provided in [Table 58 on page 298](#).

Fields marked with an asterisk (*) are mandatory.

4. Click **Traceroute** to initiate the traceroute operation.

.A job is created and a Traceroute Progress page appears. If the traceroute operation is successful, the Traceroute Result page displays the traceroute parameters specified in [Table 59 on page 299](#).

If the traceroute operation fails, the Traceroute Result page displays an appropriate error message (such as **No response** or **No route to host**).

Table 58: Fields on the Traceroute page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.

Table 58: Fields on the Traceroute page (*continued*)

Field	Description
Maximum Hops	<p>Specify the maximum number of network devices that a packet can pass through to reach the remote host.</p> <p>Default: 30.</p> <p>Range: 1 through 255.</p> <p>If the number of hops to reach the remote host exceeds the set value, the traceroute packet is dropped.</p>
Advanced	
Source Interface	<p>Select a source interface on the source device from which you want to send the packets to the remote host.</p> <p>Click Clear All to remove the selected interface and select another interface.</p>
Hostname Resolution	<p>Click the toggle button to enable or disable (default) the display of hostname of the hops in the path to the remote host.</p>
Wait Time (seconds)	<p>Enter the time until which the device waits for a response from the remote host to a packet sent before considering timeout.</p> <p>Default: 10 seconds.</p> <p>Range: 0 through 86,399 seconds.</p>
Routing Instance	<p>Select a routing instance that the traceroute request packets can use to reach the remote host.</p> <p>The trace result displays the route information based on the configured routing instance type.</p> <p>To clear the selected routing instance, click Clear All and select another routing instance.</p>

Table 59 on page 299 lists the parameters on the Traceroute Result page when the traceroute operation is successful.

Table 59: Fields on the Traceroute Result page

Field	Description
Hop	<p>Hostname or IPv4 address of the network devices that the packet passed through to reach the remote host.</p>

Table 59: Fields on the Traceroute Result page (*continued*)

Field	Description
Time Taken by Packet 1	Duration (in microseconds) between the time from when the source device sends a packet, and the time it received a response from the hops and the remote host.
Time Taken by Packet 2	
Time Taken by Packet 3	

Remotely Accessing a Device CLI

You can use the Devices page to remotely access the CLI of CPE devices, and run operational or configuration commands. To access the device CLI from the Devices page:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select a device from the list.

NOTE: You can only select a device for which the operational status is marked as **Up**.

3. Click **More > Remote Console**.

The Remote Console for *Device-Name* page appears.

NOTE: For dual SRX Series devices, the **Remote Console** option is enabled only at the cluster level and disabled at the member level.

For dual NFX250 devices, the **Remote Console** option is enabled at the individual member level and disabled at the cluster level.

4. Select one of the following options:

- **Read only access** (default option)—Allows you to automatically log in to the device through the Remote Terminal browser window, without entering a username and password. If the connection is established successfully, the operational mode CLI prompt appears in the browser window. You can run only operational commands in this mode.

- **Full access with Junos device login credentials**—Allows you to log in to the device using the Junos login credentials. If the connection is established successfully, the configuration mode CLI prompt appears in the browser window. You can run both configuration and operational commands in this mode.

5. Close the Remote Terminal browser window to disconnect from the device.

The session times out if the session remains idle for more than 15 minutes (default) and you are automatically logged out of the device. The **Remote console connection was closed. Please close this window and open the remote console again** message appears in the browser window.

You must close the idle terminal window before opening a new terminal window.

CSO generates an audit log each time a user accesses the device CLI. The logs provide information about the user, the date and time of access, and type of access (read-only or read-write). Use the Audit Logs page (**Administration > Audit Logs**) to view the remote console audit logs.

View the Current Configuration on a Device

To view the current configuration on the device:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click a device from the list.

NOTE: You can only select a device for which the operational status is marked **Up**.

3. Click the **Configuration** tab.

The Interfaces, Zones, and Running Configuration tabs appear.

4. Click the **Running Configuration** tab.

The configuration that is currently running on the device is displayed. You can view the configuration either as CLI or text.

To remotely access the device CLI, click the **Remote Console** option. The Remote Terminal browser window appears, displaying the **CONNECTING TO DEVICE. PLEASE WAIT FOR PROMPT** message.

You can automatically log in to the device through the Remote Terminal browser window, without entering a username and password. If you access the device CLI through the remote terminal, root user login is disabled.

NOTE: For dual SRX Series devices, the **Remote Console** option is enabled only at the cluster level and disabled at the member level.

For dual NFX250 devices, the **Remote Console** option is enabled at the individual member level and disabled at the cluster level.

- If the connection is successfully established, the CLI prompt appears in the browser window. You can use the **show** operational commands to monitor a device, verify system operation, view details of specific components on a device, and so on.
- If the connection is not established, the **Remote console connection was closed. Please close this window and open the remote console again** message appears in the browser window.

NOTE: The session times out if the session remains idle for more than 15 minutes (default) and you are automatically logged out of the device. The **Remote console connection was closed. Please close this window and open the remote console again** message appears on the browser window.

You must close the idle terminal window before opening a new terminal window.

Generate Device RSI for Enterprise Hub and Spoke Devices

Starting from Release 6.0.0, CSO provides the option to generate the device RSI (request support information) file. Before you contact the customer support team, you must generate an RSI file for the device. The RSI file contains system data that can be analyzed to troubleshoot and debug any issue.

Only the SP administrator, OpCo administrator, or tenant administrator can generate the device RSI. Users with custom roles can generate RSI files, if the device RSI action is enabled for that role.

You can generate the device RSI log file for NFX150, NFX250, SRX Series, and vSRX devices. To generate the RSI log, the operational status of the device must be UP.

To collect the device RSI:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select a device from the list of devices displayed and click **More > Device RSI**. You can generate the device log for only one device at a time.

An alert message that prompts you to confirm the operation appears.

3. Click **Yes**.

A message indicating that the request system information job is triggered is displayed. You can click the link in the message to view the progress of the job. Alternatively, you can view the progress on the Jobs (**Monitor > Jobs**) page.

If the job is completed successfully, a confirmation message appears. This job might take up to 35 minutes to complete depending on the device type.

You can download the log file from the Jobs page. To download the device log, click the **[Download Logs]** link next to the job name. The log file is saved in a compressed (.gz) format with the **rsi_site-name_JUNOS** filename. Extract the file to view the details. For the NFX250 device, CSO generates separate RSI files for Juniper Device Manager (JDM), Junos Control Plane (JCP), and gateway router (GWR).

NOTE: CSO retains only one version of the log file. Each time you generate a log file, the previous version is overwritten.

Configuring the Firewall Device

Zones, physical interfaces, and routing instances are the basic building blocks of firewall policy and NAT policy. You can configure them from the **Resources > Devices > Device-Name > Configuration** page.

NOTE: The **Configuration** tab that was available in earlier releases for stage-2 template-based configuration is renamed as **Configuration Template**.

To configure the firewall device:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The physical interfaces, routing instances, and zones tabs appear.

4. Complete the configuration settings according to the guidelines provided in [Table 60 on page 304](#).

5. Click **OK** to save the changes.

The newly created physical interfaces, routing instances, and zones are displayed in the relevant tabs in the Configurations page.

Table 60: Fields on the Device Configuration Page

Field	Description
Physical Interfaces	
Interface Name	Name of the physical interface on the device.
Logical Interfaces	<p>Click View/Configure to view or configure the logical interfaces associated with the physical interface on the device.</p> <p>To view and add logical interfaces for a physical interface, see “About the Logical Interfaces Page” on page 306 and “Adding a Logical Interface” on page 307.</p>
Zones	
Name	<p>Name of the zone that you use for firewall policies and NAT policies.</p> <p>To add a new security zone, see “Adding a Security Zone” on page 318.</p>
Interfaces	Interfaces associated with the zone.
Screen	Screen name for the security zone.
Description	Description for the zone.

Table 60: Fields on the Device Configuration Page (*continued*)

Field	Description
Routing Instances	
Name	Name of the routing instances for security configuration. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters.
Static Route	Click View/Configure to view or configure the static routes associated with a routing instance on the device.
Interfaces	Name of the interface over which the traffic flows.
Instance Type	Type of routing instance.
Description	Description of the routing instance.

About the Physical Interfaces Page

To access this page, click **Resources > Devices > Device-Name > Configuration**.

Use this page to view or edit the physical interfaces on the device. You can also view and configure the logical interfaces associated with the physical interfaces.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the physical interfaces. Click the **View/Configure** button to view or configure the logical interfaces for the physical interface. See [“About the Logical Interfaces Page” on page 306](#).
- Show or hide columns about the physical interface. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a physical interface. Click the Search icon in the top right corner of the page to search for an interface.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

Table 61 on page 306 shows the fields on the Physical Interface page.

Table 61: Fields on the Physical Interface Page

Field	Description
Interface Name	Name of the physical interface on the device.
Logical Interfaces	Click View/Configure to view or configure the logical interfaces associated with the physical interface on the device. To view and add logical interface for a physical interface, see “About the Logical Interfaces Page” on page 306 and “Adding a Logical Interface” on page 307 .
MTU	Maximum transmission unit (MTU) size (in bytes) on the physical interface.
Speed	Speed in gigabytes per second (Gbps), at which data is transferred for the physical interface.
Description	Description of the physical interface.

About the Logical Interfaces Page

To access this page, click **Resources > Devices > Device-Name > Configuration > Physical Interfaces > View/Configure**.

Use this page to view, create, edit, or delete logical interfaces associated with a physical interface on the device.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the logical interfaces. See [Table 62 on page 307](#) for descriptions of the fields on the logical interfaces page.
- Add a logical Interface. See [“Adding a Logical Interface” on page 307](#).
- Edit, delete, or deploy logical interfaces. See [“Editing, Deleting, and Deploying Logical Interfaces” on page 310](#).

- Clear all selected logical interfaces. Select the logical interface and then right-click or click **More > Clear All Selections**.
- Show or hide columns that contain information about the logical interface. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for logical interfaces using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

[Table 62 on page 307](#) shows the fields on the Logical Interfaces page.

Table 62: Fields on the Logical Interfaces Page

Field	Description
Interface Name	Displays the name of the logical interface associated with a physical interface on the device.
IPv4 Address	Displays the IPv4 address for the logical interface..
IPv6 Address	Displays the IPv6 address for the logical interface.
VLAN ID	Displays the VLAN ID for the 802.1q VLAN tags.
Description	Displays the description of the logical interface.

Adding a Logical Interface

For a physical interface to function, you must configure at least one logical interface on that device. . You can also configure other logical interface properties.

The logical properties of an interface are the characteristics that do not apply to the physical interface. Logical properties include:

- IP address or addresses associated with the interface. A logical interface can be configured with an IPv6 address, IPv4 address, or both. The IP specification requires a unique address on every interface of each system attached to an IP network, so that traffic can be correctly routed. Individual hosts such as home computers must have a single IP address assigned. Devices must have a unique IP address for every interface.
- Virtual LAN (VLAN) tagging

To create logical interface for a physical interface:

1. Select **Resources > Devices** .

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

4. Click **Physical Interfaces** tab.

The Physical Interfaces page appears.

5. Select a physical interface and click **View/Configure**.

The Logical Interfaces page appears.

6. Click the plus icon (+) .

The Create Logical Interface page appears.

7. Complete the configuration settings according to the guidelines provided in [Table 63 on page 308](#).

8. Click **OK** to save the changes.

Table 63: Fields on the Logical Interfaces Page

Field	Description
Basic Information	
Unit	Enter the number of the logical interface. Range: 0 through 2,147,483,647.
Description	Enter a description for the logical interface. The maximum number of characters is 255.
VLAN ID	Enter the VLAN ID for the 802.1q VLAN tags.
IPv4 Address	Click the plus icon (+) . The Add - Address(IPv4) page appears.

Table 63: Fields on the Logical Interfaces Page (*continued*)

Field	Description
IPv4 Address	Enter an IPv4 address for the logical interface.
Subnet	Enter the subnet for the IPv4 address. Range: 0 through 32
Primary	Select this check box to mark the IPv4 address as the primary address of the protocol on the logical interface. If the logical unit has more than one IP address, the primary IP address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.
Preferred	Select this check box to specify that the IPv4 address is the preferred address for the logical interface. If you configure more than one IP address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet.
IPv6 Address	Click the plus icon (+) . The Add - Address(IPv6) page appears.
IPv6 Address	Enter an IPv6 address for the logical interface.
Subnet	Enter the subnet for the IPv6 address. Range: 0 through 32
Primary	Select this check box to specify that the IPv6 address is the primary address of the protocol on the logical interface. If the logical unit has more than one IP address, the primary IP address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.
Preferred	Select this check box to specify that the IPv6 address is the preferred address for the logical interface. If you configure more than one IP address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet.

Editing, Deleting, and Deploying Logical Interfaces

IN THIS SECTION

- [Editing Logical Interfaces | 310](#)
- [Deleting Logical Interfaces | 311](#)
- [Deploying Logical Interfaces | 311](#)

You can edit, delete, and deploy logical interfaces from the **Logical Interfaces** page.

Editing Logical Interfaces

To modify the parameters configured for a logical interface:

1. Select **Resources > Devices > Device-Name > Configuration > Physical Interface > View/Configure**.

The **Logical Interfaces** page appears.

2. Select the logical interface that you want to edit, and then click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit**.

The **Edit Logical Interface** page appears.

3. Modify the parameters according to the guidelines provided in [“Adding a Logical Interface” on page 307](#).

NOTE: You can modify only some fields when you are editing a logical interface.

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the modified values appear on the **Logical Interfaces** page.

Deleting Logical Interfaces

To delete a logical interface:

NOTE: You cannot delete a logical interfaces that is associated with a physical interface on the device.

1. Select **Resources > Devices > Device-Name > Configuration > Physical Interface > View/Configure**.
The **Logical Interfaces** page appears.
2. Select one or more logical interfaces that you want to delete and then click the delete icon.
A page requesting confirmation for the deletion appears.
3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected logical interface is deleted from the **Logical Interfaces** page.

Deploying Logical Interfaces

To deploy a logical interface:

1. Select **Resources > Devices > Device-Name > Configuration > Physical Interface > View/Configure**.
The **Logical Interfaces** page appears.
2. Select one or more logical interfaces that you want to deploy and then click **Deploy**.
A job is created. Click the job link or go to the Jobs page and view the status of the deployment.

RELATED DOCUMENTATION

| [Adding a Logical Interface](#) | 307

Enable LLDP on a CPE Interface

To discover a switch or access point (AP) connected to an SRX Series Customer Premise Equipment (CPE), enable Link Layer Discovery Protocol (LLDP) on the CPE interface used.

LLDP allows networked devices to advertise capabilities, identity, and other information onto a LAN. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices.

If you are using a LAG or a reth interface to connect to a switch or an AP, you can enable LLDP on the interface when you create the interface (see [“Create LAG Interface” on page 312](#) and [“Create a RETH Interface” on page 314](#))

To enable LLDP on a CPE interface:

1. Click **Resources > Devices**.

The Devices page is displayed.

2. Select a CPE from the list of devices displayed and click **More > Manage Switch Connectivity**.

The **Manage Switch Connectivity** page is displayed.

Alternatively, click *device-name* from the **Device Name** column to open the **Device Details** page and then click **Configuration (tab) > Interfaces (tab)**.

You can also access the **Device Details** page from the Site Management page (**Resources > Site Management *site-name* > DEVICES (tab) > *device-name***).

NOTE: You can enable LLDP on a device only if the Management Status of the selected device is **Provisioned**.

3. Select the interface from the Interfaces section and click the edit (pencil) icon.

The **Edit *interface-name*** page is displayed.

4. Click the toggle button against the **LLDP** field to enable LLDP.

5. Click **OK**.

Create LAG Interface

You can connect an SRX Series Customer Premise Equipment (CPE) to an EX series switch or an access point (AP) through a trunk port. However, you can use two or more trunk ports to connect the CPE and the switch, and combine them to form a Link Aggregation Group (LAG) for higher throughput and redundancy. If you want to use a LAG interface to manage the connectivity between the CPE and the switch, create a LAG interface (aggregated Ethernet or ae interface) on the CPE.

To create a LAG interface:

1. Click **Resources > Devices**.

The **Devices** page is displayed.

2. Select a CPE device from the list of devices displayed and click **More > Manage Switch Connectivity**.

The **Manage Switch Connectivity** page is displayed. To access this page, the Management Status of the device selected should be **Provisioned**.

Alternatively, click *device-name* from the **Device Name** column to open the **Device Details** page and then click **CONFIGURATION (tab) > Interfaces (tab)**.

You can also access the **Device Details** page from the Site Management page (**Resources > Site Management *site-name* > DEVICES (tab) > *device-name***).

3. Click **Add LAG Interface**.

The **Create LAG Interface** page is displayed.

4. Complete the configuration settings according to the guidelines provided in [Table 64 on page 313](#).

5. Click **OK**.

The LAG interface is listed in the interfaces section on the **Manage Switch Connectivity** page.

Table 64: Fields on the Add LAG Interface Page

Field	Description
LAG Interface	Select a LAG interface. This must be an Aggregated Ethernet (ae) interface.
CPE Port(s)	Select the physical interfaces (of the CPE) to be included as the member links in the LAG. These interfaces are used for data or management traffic between the EX Series switch and the CPE. Select at least two ports for redundancy.
LACP	Enable Link Aggregation Control Protocol (LACP), a monitoring protocol that detects link-layer failure within a network, if you want to monitor the local and remote ends of member links in a LAG.
Setting	<p>If you have enabled LACP on the interface, select the LACP mode.</p> <ul style="list-style-type: none"> • Active—To initiate transmission of LACP packets and response to LACP packets, you must configure LACP in active mode. If either the actor (transmitting link) or partner (receiving link) is active, they exchange LACP packets. • Passive—There is no exchange of LACP packets. This is the default transmission mode.

Table 64: Fields on the Add LAG Interface Page (*continued*)

Field	Description
Interval	<p>If you have enabled LACP on the interface, select an interval for periodic transmission of LACP packets:</p> <ul style="list-style-type: none"> • fast—Transmits packets every second. • slow—Transmits packets every 30 seconds.
Force up	<p>If you have enabled LACP on the interface, click the toggle button if you want to enable the Force Up state on the interface. Enabling this feature sets the state of the interface as UP even when the peer has limited LACP capability.</p>
LLDP	<p>Use the toggle button to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP allows networked devices to advertise capabilities, identity, and other information onto a LAN. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices.</p>

Create a RETH Interface

For an SD-WAN site with dual CPE cluster, you can use a redundant Ethernet (reth) interface to connect the SRX Series Customer Premise Equipment (CPE) devices to an EX Series switch or an access point (AP). A redundant Ethernet (reth) interface is a pseudo-interface that includes a physical interface from each node of a cluster. The reth interface of the active node is responsible for passing the traffic in a chassis cluster setup.

To create a reth interface:

1. Click **Resources > Devices**.

The **Devices** page is displayed.

2. Select a CPE device from the list of devices displayed and click **More > Manage Switch Connectivity**.

The **Manage Switch Connectivity** page is displayed. To access this page, the Management Status of the selected device should be **Provisioned**.

Alternatively, click *device-name* from the **Device Name** column to open the **Device Details** page and then click **CONFIGURATION (tab) > Interfaces (tab)**.

You can also access the **Device Details** page from the Site Management page (**Resources > Site Management *site-name* > DEVICES (tab) > *device-name***).

3. Click **Add RETH Interface**.

The **Create RETH Interface** page is displayed.

4. Complete the configuration settings according to the guidelines provided in [Table 65 on page 315](#).
5. Click **OK**.

The RETH interface is listed on the Interfaces section of the page.

Table 65: Fields on the Add RETH Interface Page

Field	Description
RETH Interface	Select a reth interface from the list.
CPE Node 0 Port(s)	Select the physical interfaces (of the Node 0) to be assigned to the reth interface. These interfaces are used for data or management traffic between the switch and the CPE.
CPE Node 1 Port(s)	Select the physical interfaces (of the Node 1) to be assigned to the reth interface. These interfaces are used for data or management traffic between the switch and the CPE.
Redundancy Group	Select a redundancy group you want to associate this reth interface with. Alternatively, click Create Redundancy Group to create a redundancy group.
LACP	Enable Link Aggregation Control Protocol (LACP), a monitoring protocol that detects link-layer failure within a network, if you want to monitor the local and remote ends of member links (physical interfaces) in a reth interface.
Setting	<p>If you have enabled LACP on the interface, select the LACP mode:</p> <ul style="list-style-type: none"> • Active—To initiate transmission of LACP packets and response to LACP packets, you must configure LACP in active mode. If either the actor (transmitting link) or partner (receiving link) is active, they exchange LACP packets. • Passive—There is no exchange of LACP packets. This is the default transmission mode.
Interval	<p>If you have enabled LACP on the interface, select an interval for periodic transmission of LACP packets from the following options:</p> <ul style="list-style-type: none"> • fast—Transmits packets every second. • slow—Transmits packets every 30 seconds.
Force up	If you have enabled LACP on the interface, click the toggle button to enable the Force Up state on the interface. Enabling this feature sets the state of the interface as UP even when the peer has limited LACP capability.

Table 65: Fields on the Add RETH Interface Page (*continued*)

Field	Description
LLDP	Use the toggle button to enable Link Layer Discovery Protocol (LLDP) on the interface. LLDP allows networked devices to advertise capabilities, identity, and other information onto a LAN. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices.

Create a Redundancy Group

A redundancy group is an abstract construct that includes and manages a collection of objects on both nodes of a chassis cluster. A redundancy group is primary on one node and backup on the other node at any given time. Each redundancy group fails over from one node to the other independent of other redundancy groups. When a redundancy group fails over, all its objects fail over together.

Three things determine the primacy of a redundancy group: the priority configured for the node, the node ID (in case of tied priorities, the node with the lowest node ID number takes precedence), and the order in which the node comes up. If a lower priority node comes up first, it assumes the primacy for a redundancy group (and stays as primary if preempt is not enabled). If preempt is added to a redundancy group configuration, the device with the higher priority in the group can initiate a failover to become primary.

To create a redundancy group:

1. Click **Resources > Devices**.

The **Devices** page is displayed.

2. Click the *device-name* from the **Device Name** column to open the **Device Details** page and then click **CONFIGURATION (tab) > Redundancy Group (tab)**.

The **Redundancy Group** page is displayed.

You can also access the **Device Details** page from the Site Management page (**Resources > Site Management *site-name* > DEVICES (tab) > *device-name***).

3. Click the + button to add a new redundancy group.

Alternatively, click **Create Redundancy Group** link on the **Create RETH Interface** page. See [“Create a RETH Interface” on page 314](#) for more details.

The **Add Redundancy Group** page is displayed.

4. Complete the configuration settings according to the guidelines provided in [Table 66 on page 317](#).
5. Click **OK**.

The redundancy group is listed on the **Redundancy Group** page.

Table 66: Fields on the Add Redundancy Group Page

Field	Description
Name	Select a unique identifier for the redundancy group.
Node 0 Priority	Enter the priority value of the node 0. The eligible node with the highest priority is elected master.
Node 1 Priority	Enter the priority value of the node 1. The eligible node with the highest priority is elected master.
Preempt	<p>Enable preempt to allow the device with the higher priority in the group to initiate a failover to become primary.</p> <p>NOTE: You cannot enable preemption for redundancy group 0.</p>

Manage Redundancy Groups

To access the **Redundancy Group** tab, click **Resources > Devices > *device-name* > CONFIGURATION (tab) > Redundancy Group (tab)**.

From the **Redundancy Group** page, you can add, edit or delete a redundancy group. See also: [“Create a Redundancy Group” on page 316](#).

To edit a redundancy group:

1. Click **Resources > Devices**.

The **Devices** page is displayed.

2. Click the *device-name* from the **Device Name** column to open the **Device Details** page and then click **CONFIGURATION (tab) > Redundancy Group (tab)**.

The Redundancy Group page is displayed.

You can also access the **Device Details** page from the Site Management page (**Resources > Site Management *site-name* > DEVICES (tab) > *device-name***).

3. Select the redundancy group from the list and then click the edit (pencil) icon.

The **Edit Redundancy Group** page is displayed.

4. Make the required changes. See [“Create a Redundancy Group” on page 316](#) for details.

5. Click **OK**.

To edit a redundancy group:

1. Click **Resources > Devices**.

The **Devices** page is displayed.

2. Click the *device-name* from the **Device Name** column and then click **CONFIGURATION (tab) > Redundancy Group (tab)**.

The Redundancy Group page is displayed.

3. Select the redundancy group from the list and then click the delete icon.

A window requesting confirmation for the deletion appears.

4. Click **Yes**.

The selected redundancy group is deleted.

Adding a Security Zone

A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound. You can define multiple security zones, the exact number of which you determine based on your network needs.

An interface for a security zone can be thought of as a doorway through which TCP/IP traffic can pass between that zone and any other zone. Through the policies you define, you can permit traffic between zones to flow in one direction or in both. With the routes that you define, you specify the interfaces that traffic from one zone to another must use. Because you can bind multiple interfaces to a zone, the routes you chart are important for directing traffic to the interfaces of your choice. An interface can be configured with an IPv4 address, IPv6 address, or both.

Security zones have the following properties:

- Policies—Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall.
- Screens—A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful.
- TCP-RST—When this feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYNchronize flag set.
- Interfaces—List of interfaces in the zone.

Use this page to configure zones and assign interfaces to them.

To create a security zone:

1. Select **Resources > Devices** .

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

4. Click **Zones** tab.

The Zones page appears.

5. Click the plus icon (+) .

The Add New Zone page appears.

6. Complete the configuration settings according to the guidelines provided in [Table 67 on page 319](#).

7. Click **OK** to save the changes.

Table 67: Fields on the Add New Zone Page

Field	Description
General Information	

Table 67: Fields on the Add New Zone Page (*continued*)

Field	Description
Name	Enter a unique string of alphanumeric characters, and some special characters, such as dashes, and underscores. The maximum length is 31 characters.
Description	Enter a description for the zone; the maximum length is 900 characters.
Application Tracking	Select the checkbox to maintain application usage statistics on a device.
Interfaces	From the list of interfaces in the Available column, select the interfaces that you want to include in the new zone and click the greater-than icon (>). The selected interfaces are moved to the Selected column.
System Services	From the list of system services in the Available column, select the system services that you want to include in the new zone and click the greater-than icon (>). The selected system services are moved to the Selected column.
Is Except	Select the checkbox to disable specific incoming system service traffic, only when all system services option is defined.
Protocols	From the list of protocols in the Available column, select the protocols that you want to include in the new zone and click the greater-than icon (>). The selected protocols are moved to the Selected column.
Is Except	Select this option to disable specific incoming protocol traffic, only when all protocols option is defined.
Traffic Control Options	
TCP RST	Select the checkbox to enable sending TCP packets with the RST (reset) flag set to 1 in response to TCP packets with any flag other than SYN set and that do not belong to an existing session.
Screen	Enter a predefined security screen for a security zone to detect and block various kinds of traffic that the device determines as potentially harmful.
Interface Services and Protocols	View the summary of interface, services and protocols for your device.

Adding a Routing Instance

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables, and the routing protocol parameters control the information in the routing tables. There can be multiple routing tables for a single routing instance—for example, unicast IPv4, unicast IPv6, and multicast IPv4 routing tables can exist in a single routing instance. Routing protocol parameters and options control the information in the routing tables.

Each routing instance consists of sets of the following:

- Routing tables
- Interfaces that belong to these routing tables (optional, depending upon the routing instance type)
- Routing option configurations

You can configure the following routing instances:

- Forwarding—Use this routing instance type for filter-based forwarding applications. For this instance type, there is no one-to-one mapping between an interface and a routing instance. All interfaces belong to the default instance inet.0.
- Virtual router—Use this for non-VPN-related applications. There are no virtual routing and forwarding (VRF) import, VRF export, VRF target, or route distinguisher requirements for this instance type.

To create a routing instance:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

4. Click **Routing Instances** tab.

The Routing Instances page appears.

5. Click the plus icon (+).

The Create Routing Instance page appears.

6. Complete the configuration settings according to the guidelines provided in [Table 68 on page 322](#).
7. Click **OK** to save the changes.

Table 68: Fields on the Create Routing Instance Page

Field	Description
General Settings	
Name	Enter a unique string of alphanumeric characters, dashes, and underscores. The maximum length is 31 characters.
Description	Enter a description for the zone; the maximum length is 900 characters.
Instance Type	Select the routing instance type from the list. Select virtual-router for non-VPN-related application. Select forwarding for filter-based forwarding applications where interfaces are not associated with instances.
Interfaces	From the list of interfaces in the Available column, select the interfaces that you want to include in the new routing instance and click the greater-than icon (>). The selected interfaces are moved to the Selected column.

Create Management Connectivity Between a CPE and a Switch

To set up management connectivity between an SRX Series Customer Premise Equipment (CPE) and an EX Series switch or an access point (AP), create a zone-based LAN segment and include the CPE port (to be connected to the switch or AP) in it. This LAN segment is associated with a security zone for underlay breakout. If you have configured a LAG interface to manage the connectivity to the switch, you can add the Aggregated Ethernet (ae) interface to the LAN. This step creates reachability between the EX Series switch and Juniper Mist.

To create management connectivity between a CPE and an EX Series switch or an AP:

1. Click **Resources > Devices**.
2. Select a CPE from the list of devices displayed and click **More > Manage Switch Connectivity**.

The **Manage Switch Connectivity** page is displayed.

NOTE: You can configure the management connectivity on a CPE only if its Management Status is **Provisioned**.

3. On the right side of the **Management Connectivity** section, click the + icon.

The **Create Management Pool** page is displayed.

Alternatively, you can create a management pool (zone-based LAN segment) from the Add LAN Segment screen (**Resources > Site Management > site-name > LAN** (tab) > +). When you create a LAN segment, disable the **Use for Overlay VPN** option to associate the LAN segment with a security zone for underlay breakout.

4. Complete the configuration settings according to the guidelines provided in [Table 69 on page 323](#).

5. Click **OK**.

The LAN segment is added to the list in the **Management Connectivity** section on the **Manage Switch Connectivity** page.

On clicking **OK**, CSO applies the configuration and displays the switch or AP connected to the CPE in the Device Name column on **Devices** page (**Resources > Devices**), if a switch or an AP is already connected to the CPE. Also, the **Connected Switches** column in the Sites List on the Site Management page displays the number of switches connected to the CPE.

To view a switch or an AP which is connected to a CPE at a later time (after the Management Pool was created), select the CPE from the Device page and click **Discover Connected Device**.

Table 69: Fields on the Create Management Pool page

Field	Description
Name	Enter a name for the LAN segment.
CPE Port	Select the CPE port to be added to the management pool (the zone-based LAN segment). If you are using a LAG interface to connect the CPE to the switch or an AP, select an aggregated Ethernet (ae) interface. In case of dual CPE deployments, you can select a reth interface. NOTE: Ensure that you have enabled LLDP on the interface selected.
VLAN ID	Specify a VLAN ID for this LAN Segment. By default, VLAN ID is set to 1 and native VLAN is enabled for untagged traffic.

Table 69: Fields on the Create Management Pool page (*continued*)

Field	Description
Use for Native VLAN	Enable this option to use the specified VLAN ID for untagged traffic. The CPE interface is configured with a native-vlan-id, which has the same value as the VLAN ID.
Gateway Address/Mask	<p>Enter a valid gateway IP address and mask for the LAN segment. This address will be the default gateway for endpoints in this LAN segment.</p> <p>For example: 192.0.2.8/24.</p>
Zone	Select a security zone to be associated with this LAN segment. Alternatively click Create Zone to create a new security zone and assign that to this LAN segment. See “Adding a Security Zone” on page 318 for details.
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP.</p> <p>You can enable DHCP if you want to assign IP addresses by using a DHCP server or disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p>NOTE: If you enable DHCP, additional fields appear on the page.</p>
Additional fields related to DHCP	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	<p>Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server.</p> <p>Default: 1440</p> <p>Range: 0 through 4,294,967,295 seconds.</p>
Name Server	<p>Specify one or more IPv4 addresses of the DNS server.</p> <p>To enter more than one DNS server address, type the address, press Enter, and then type the next address.</p> <p>NOTE: DNS servers are used to resolve hostnames into IP addresses.</p>

Discover an EX Series Switch or APs Configured Behind a CPE

NOTE: To discover an EX Series switch or an access point (AP) connected to an SRX Series Customer Premise Equipment (CPE) device, you must enable LLDP on the CPE device interface to be connected to the switch or the AP.

On completing configuration of a zone-based LAN segment for providing management connectivity between a CPE and a switch or an AP, CSO applies the configuration and displays the switch connected to the CPE on the Site Management page and Device page, if a switch is already connected to the CPE.

To view a switch or an AP which is connected to a CPE at any time, use the following steps:

1. Click **Resources > Devices**.

The Devices page is displayed.

2. Select the CPE from the list and click **Discover Connected Device**.

CSO displays the switch or the AP connected to the CPE in the **Device Name** column on **Devices** page (**Resources > Devices**).

CSO also displays the number of switches connected to the CPE in **Connected Switches** column on **Site Management** page (**Resources > Site Management**).

View an EX Series Switch or an AP on Mist

After CSO discovers an EX Series switch or an access point (AP) that is connected to an SRX Series Customer Premise Equipment (CPE), you can launch the Mist portal from the Devices page to view the details of the switch. You can view information such as device metrics, properties, statistics, and configuration.

To launch the Mist portal from the Devices page:

1. Click **Resources > Devices**.

The **Device** page is displayed.

Alternatively,

- a. Click **Resources > Site Management**.
- b. Click the site name in the **Site Name** column on the **Site Management** page.

- c. Click the **Devices** tab.

The list of devices added to the site appears.

2. Click the *EX Series switch* in the **Device Name** column on the **Devices** page.

You are redirected to the Mist portal.

View an SRX Series CPE on Juniper Mist

You can view the details of an SRX Series Customer Premise Equipment (CPE) that is added to the Juniper Mist platform. You can view information such as device metrics, properties, statistics, and configuration.

To view the information about an SRX Series CPE on Mist:

1. Click **Resources > Devices**.

The **Device** page is displayed.

2. Select the SRX Series device from **Devices** page and click **WAN Assurance**.

You are redirected to the Mist page for the selected SRX Series device.

NOTE: The SRX Series device selected must be added to the Mist platform.

About the Static Routes Page

To access this page, click **Resources > Devices > Device-Name > Configuration > Routing Instances > View/Configure**.

Use this page to view, create, edit, or delete static routes for the routing instance.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the static route. See [Table 70 on page 327](#) for descriptions of the fields on the static routes page.
- Add a static route. See [“Adding a Static Route” on page 327](#).

- Edit, delete, or deploy static routes. See [“Editing, Deleting, and Deploying Static Routes” on page 330](#).
- Clear all selected static routes. Select the static route and then right-click or click **More > Clear All Selections**.
- Show or hide columns that contain information about the static route. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for static routes using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

[Table 70 on page 327](#) shows the fields on the Static Routes page.

Table 70: Fields on the Static Routes Page

Field	Description
IP Address	View the IP address of the static route.
Next Hop	View the Ipv4 or IPv6 address for the next hop.
Next Table	View the name of the next routing table to the destination.
Metric	View the metric value that signifies the cost for an access route, for the next hop
Status	View the status of the static route.

Adding a Static Route

Routes that are permanent fixtures in the routing and forwarding tables are often configured as static routes. These routes generally do not change, and often include only one or very few paths to the destination.

To create a static route in the routing table, you must, at minimum, define the route as static and associate a next-hop address with it. The static route in the routing table is inserted into the forwarding table when the next-hop address is reachable. All traffic destined for the static route is transmitted to the next-hop address for transit.

NOTE: This workflow is applicable only for next-generation firewall sites. For other sites, you can add static routes through configuration templates.

You can specify options that define additional information about static routes that is included with the route when it is installed in the routing table. All static options are optional.

To create a static route for a routing instance:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

4. Click **Routing Instances** tab.

The Routing Instances page appears.

5. Select a routing instance and click **View/Configure** link in the **Static Route** column.

The Static Routes page appears.

6. Click the plus icon (+) .

The Create Static Route page appears.

7. Complete the configuration settings according to the guidelines provided in [Table 71 on page 328](#).

8. Click **OK** to save the changes.

Table 71: Fields on the Create Static Route Page

Field	Description
Basic Information	
IP Address	Enter the IPv4 or IPv6 address depending on the type of IP address specified.
Subnet	Enter the subnet for the IPv4 address or the prefix for the IPv6 address.

Table 71: Fields on the Create Static Route Page (*continued*)

Field	Description
Next Hop	
IP Address	Enter an IPv4 or IPv6 address for the next hop depending on the type of IP address specified for the static route.
Interface	Select the interface name to be used as the next hop.
Qualified Next Hop	
IP Address	Enter an IPv4 or IPv6 address for the qualified next hop depending on the type of IP address specified for the static route.
Interface	Select the interface name to be used as the qualified next hop.
Preference	Enter the preference for the qualified next hop; the lower the number, the higher the route preference.
Metric	Enter a metric value to signify the cost for an access route for the qualified next hop.
Next Table	
Next Table	Select the name of the next routing table to the destination.
Advanced Options	
Preference	Enter the preference for the next hop; the lower the number, the higher the route preference. Range: 0 through 2147483647
Metric	Enter a metric value which signifies the cost for an access route, for the next hop Range: 0 through 2147483647
Discard	Specify whether to drop packets to destination; send no ICMP unreachable
Resolve Choices	Select whether indirectly connected next hops must be resolved (Resolve) or not (Do not resolve). Select None if no action is required.
Retain Choices	Select whether the route must be retained (Retain) or deleted from the forwarding table (Do not retain) when the routing protocol process shuts down normally. Select None if no action is required.

Table 71: Fields on the Create Static Route Page (*continued*)

Field	Description
Install Choices	Select whether the route must be installed in the forwarding table (Install) or not (Do not install). Select None if no action is required.
Re-advertise Choices	Select whether the route must be re-advertised by routing protocols (Re-advertise) or not (Do not re-advertise). Select None if no action is required.

Editing, Deleting, and Deploying Static Routes

IN THIS SECTION

- [Editing Static Routes | 330](#)
- [Deleting Static Routes | 331](#)
- [Deploying Static Routes | 331](#)

You can edit, delete, and deploy static routes from the **Static Routes** page.

Editing Static Routes

To modify the parameters configured for a static route:

1. Select **Resources > Devices > Device-Name > Configuration > Routing Instances > View/Configure**.

The **Static Routes** page appears.

2. Select the static route that you want to edit, and then click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit**.

The **Edit static route** page appears.

3. Modify the parameters according to the guidelines provided in [“Adding a Static Route” on page 327](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the modified values appear on the **Static Routes** page.

Deleting Static Routes

To delete a static route:

1. Select **Resources > Devices > *Device-Name* > Configuration > Routing Instances > View/Configure**.

The **Static Routes** page appears.

2. Select one or more static routes that you want to delete and then click the delete icon.

A page requesting confirmation for the deletion appears.

3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected static route is deleted from the **Static Routes** page.

Deploying Static Routes

To deploy a static route:

1. Select **Resources > Devices > *Device-Name* > Configuration > Routing Instances > View/Configure**.

The **Static Routes** page appears.

2. Select one or more static routes that you want to deploy and then click **Deploy**.

A job is created. Click the job link or go to the Jobs page and view the status of the deployment.

RELATED DOCUMENTATION

| [Adding a Static Route](#) | 327

Managing Device Templates

IN THIS CHAPTER

- [Device Template Overview | 332](#)
- [About the Device Template Page | 337](#)
- [Cloning a Device Template | 340](#)
- [Importing a Device Template | 341](#)
- [Updating Stage-2 Configuration Template in a Device Template | 343](#)
- [Configuring Stage-2 Initial Configuration in a Device Template | 348](#)

Device Template Overview

IN THIS SECTION

- [Platform | 333](#)
- [SD-WAN CPE | 333](#)
- [Secure Internet CPE | 335](#)
- [Managed Internet CPE | 336](#)

A device template contains configuration and provision settings for a physical device, such as a CPE device or a router, which you manage through Contrail Service Orchestration (CSO). The CSO installation includes several default device templates for CPE devices and other physical devices. You can either use a default CPE device template as is if the template suits your specific topology requirements or customize the default CPE device template to meet your specific requirements. You can also create your own device templates and upload that to CSO. The CPE device templates are specific to the type of device and topology of the solution. The device templates for non-CPE devices are fixed and you cannot customize them. You must assign a device template to each CPE device at the site. You assign a device template to a device in CSO when you add a point of presence (POP). In some cases, you might want all CPE devices to use the same values, through device templates, you have the options to provide the values.

NOTE: In CSO Release 5.0, device templates are owned and managed by the Juniper Networks team that manages the cloud installation of CSO. If you need to modify device templates, talk to your Juniper Networks representative.

The CPE device templates contain three types of information:

- **Template settings information**—It prepares the device for remote activation, connects the device to the peer router, and establishes an IPsec tunnel with the router.
- **Stage-2 configuration template information**—It specifies the additional settings that you or your customer can configure for the device. For example, you can enable configuration of LAN and firewall policies. You create these configuration templates in Configuration Designer and provide implementation details in the device template.
- **Stage-2 initial configuration information**—It provides the actual values for the stage-2 configuration templates. In general, your customers perform this configuration through the Customer Portal.

The CPE device templates support four deployment models: Platform, SD-WAN CPE, Secure Internet CPE, and Managed Internet CPE.

Platform

Starting in Release 6.0.0, CSO uses platform-specific templates (SRX Platform, NFX150 Platform, or Dual SRX platform) to onboard a device. These platform templates contain the basic configuration settings required for CSO to activate and manage the device.

SD-WAN CPE

You can use the **NFX 150 as SDWAN CPE**, **NFX 250 as SDWAN CPE**, **Dual NFX 250 as SDWAN CPE**, **SRX as SDWAN CPE**, **SRX-1500 as SDWAN CPE**, **SRX-4x00 as SDWAN CPE**, **Dual SRX as SDWAN CPE**, **Dual SRX 1500 as SDWAN CPE**, or **Dual SRX 4x00 as SDWAN CPE** device template for a CPE device in an SD-WAN deployment.

Figure 15 on page 334 shows the topology for an SD-WAN CPE deployment model.

Figure 15: SD-WAN CPE

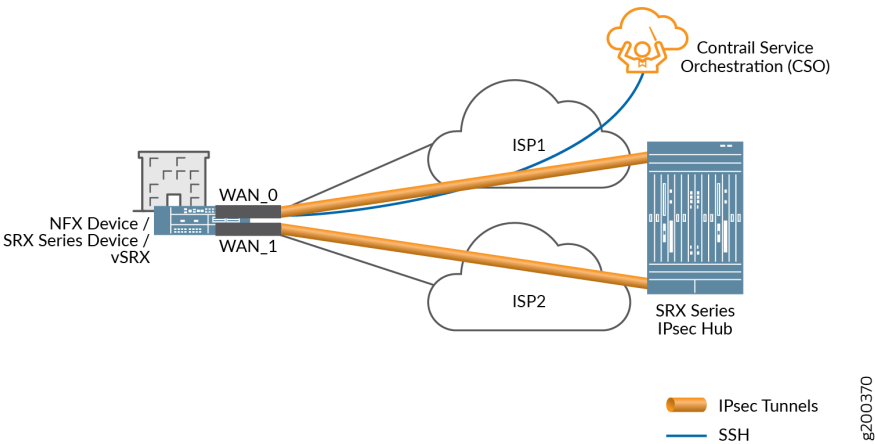


Table 72 on page 334 lists the connectivity details for an SD-WAN CPE.

Table 72: Connectivity Details for SD-WAN CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	MPLS, Internet	ge-1/0/1 (NFX150) ge-0/0/10 (NFX250) ge-0/0/0 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM
WAN_1	MPLS, Internet	ge-1/0/2 (NFX150) ge-0/0/11 (NFX250) ge-0/0/1 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM
WAN_2	MPLS, Internet	ge-1/0/3 (NFX150) (NFX1250) ge-0/0/2 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM

Table 72: Connectivity Details for SD-WAN CPE (continued)

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_3	MPLS, Internet	ge-1/0/4 (NFX150) (NFX250) ge-0/0/3 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM

Secure Internet CPE

You can use the **NFX 150 as Secure Internet CPE** or **NFX 250 as Secure Internet CPE** device template to provide a secure Internet connection through the CPE device.

Figure 16 on page 335 shows the topology for a secure Internet CPE deployment model.

Figure 16: Secure Internet CPE

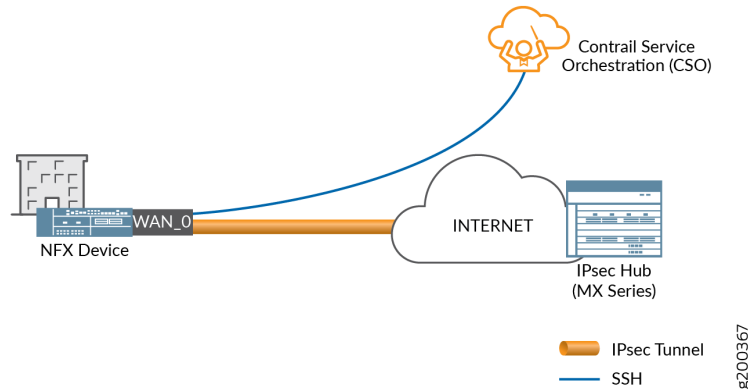


Table 73 on page 335 lists the connectivity details for secure Internet CPE.

Table 73: Connectivity Details for Secure Internet CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	Internet	ge-1/0/1 (NFX150) ge-0/0/8 (NFX250)	DHCP	IPsec	Data, OAM

Managed Internet CPE

You can use the **NFX Managed Internet CPE** or **SRX Managed Internet CPE** device template to provide a managed Internet connection through the CPE device.

Figure 17 on page 336 shows the topology for a managed Internet CPE deployment model.

Figure 17: Managed Internet CPE

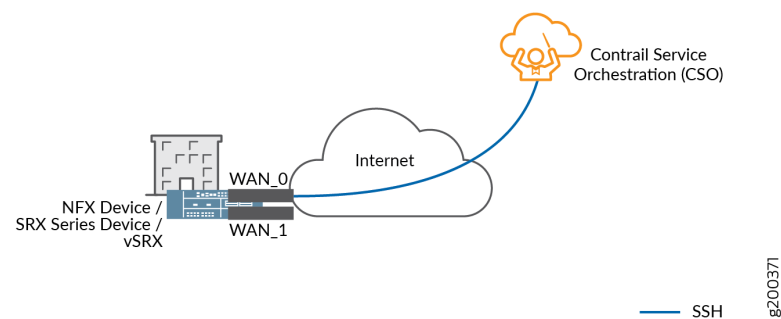


Table 74 on page 336 lists the connectivity details for a managed Internet CPE deployment model.

Table 74: Connectivity details for Managed Internet CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	Internet	ge-1/0/1 (NFX150) ge-0/0/8 (NFX250)	DHCP	—	Data, OAM

RELATED DOCUMENTATION

About the Device Template Page | 337

About the Device Template Page

IN THIS SECTION

- [Tasks You Can Perform | 337](#)
- [Field Descriptions | 337](#)
- [Supported Device Templates | 338](#)

To access this page, click **Resources > Templates > Device Templates**.

Use this page to view and manage device templates.

Tasks You Can Perform

You can perform the following tasks from this page:

- Clone a device template. See *Cloning a Device Template*.
- Import a device template from a file. See *Importing a Device Template*.
- Update stage-2 configuration template. See *Updating Stage-2 Configuration Template in a Device Template*.
- Configure stage-2 initial configuration. See *Configuring Stage-2 Initial Configuration in a Device Template*.
- View details of a device template—Hover over the device template name and Click the Detailed View icon or click **More > Detail View**.

The detailed view pane for the selected device template appears on the right side of the Device Templates page, displaying details such as the target family and tenants.

Click the close icon (X) to close the pane.

- Show or hide columns displayed on the page—Click the **Show Hide columns** icon in the top right corner of the table and select the columns that you want to view on the page.
- Search for a specific device template—Click the Search icon in the top right corner of the table and enter the search text in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 75 on page 338](#) describes the fields on the Device Templates page.

Table 75: Fields on the Device Templates Page

Field	Description
Name	Name of the device template
Description	Description of the device template. Example: NFX250 device deployed as a CPE device with SD-WAN capability.
Version	CSO version of the device template.
Build	CSO build name of the device template.
Assigned to	Number of tenant sites using the device template. Example: 2 Tenants (2 Sites)
Workflows	Number of workflows used in the device template. Example: 7
Target Family	Name of the device family for which the device template is created. Example: juniper-srx
Owner	Name of the owner (<i>OpCo Name</i> or <i>default-project</i>) who created the device template.
Last Updated	Date and time when the device template was last updated. Example: 05/23/2017 06:22

Supported Device Templates

[Table 76 on page 338](#) describes the list of supported device templates.

Table 76: List of Supported Device Templates

Device Template Name	Device Template Description
NFX250 as Managed Internet CPE	Device template for an NFX250 device acting as a CPE for a managed Internet service. This device template supports managed Internet Service with one Gigabit Ethernet WAN link.

Table 76: List of Supported Device Templates (*continued*)

Device Template Name	Device Template Description
NFX250 as SD-WAN CPE	<p>Device template for an NFX250 device acting as a CPE in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
Dual NFX250 as SD-WAN CPEs	<p>Device template for NFX250 devices in device redundancy mode in an SD-WAN deployment.</p> <p>This device template supports device redundancy in SD-WAN deployment with up to four WAN links.</p>
NFX150 as Managed Internet CPE	<p>Device template for an NFX150 device as CPE for managed Internet service. This device template supports managed Internet Service with one Gigabit Ethernet WAN link.</p>
NFX150 as SD-WAN CPE	<p>Device template for an NFX150 device as CPE in an SD-WAN deployment with hub-and-spoke topology. This device template supports up to four WAN links.</p>
SRX as SD-WAN CPE	<p>Device template for an SRX Series Services Gateway acting as a CPE device in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
SRX as SDWAN Hub	<p>Device template for an SRX Series Services Gateway acting as a hub device in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
Dual SRX as SD-WAN CPEs	<p>Device template for SRX Series Services Gateways acting as CPE devices in device redundancy mode in an SD-WAN deployment.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
vSRX as SD-WAN spoke in AWS	<p>Device template for a vSRX instance acting as spoke in AWS for SD-WAN deployment.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>

Table 76: List of Supported Device Templates (*continued*)

Device Template Name	Device Template Description
SRX-4x00 as SD-WAN CPE	<p>Device template for SRX4100, SRX4200, and SRX4600 Services Gateways acting as a CPE device in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
Dual SRX4x00 as SD-WAN CPEs	<p>Device template for SRX4100, SRX4200, and SRX4600 Services Gateways acting as CPE devices in device redundancy mode in an SD-WAN deployment.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
SRX_Standalone_Pre_Staged_NonZTP	Device template for pre-staged SRX Services Gateways acting as a Standalone CPE device without ZTP.
SRX as Security Services CPE	Device template for pre-staged SRX Services Gateways acting as a Standalone Security device with ZTP.

Cloning a Device Template

Cloning a device template is useful when you want to create a device template that is similar to an existing one but with small differences. You can clone a device template by using either of the methods mentioned below:

To clone a device template:

1. Select **Resources > Templates > Device Templates**.

The Device Template page appears.

2. Select the device template that you want to clone, and click **Clone**.

The Clone Template page appears.

3. Specify an appropriate name for your new device template. For example, SRX as SD-WAN CPE.

4. Click **Ok**.

The cloned device template appears on the Device Template page. You can now edit the new device template and customize the configurations as needed.

NOTE: You can create only one clone of a platform template. If a cloned platform template is present, then CSO uses this template to onboard the device.

You can also clone the device template by performing the following procedure:

1. Select **Resources > Templates > Device Templates**.

The Device Template page appears.

2. Select the device template that you want to clone, and then select **Edit Device Template > Template Settings**.

The Template Settings page appears.

3. Modify the configurations as required and click **Save As**.

The Create Device template page appears.

4. Specify an appropriate name for your new device template. For example, SRX as SD-WAN CPE.

5. Click **Ok**.

The cloned device template appears on the Device Template page. You can now edit the new device template and customize the configurations as needed.

RELATED DOCUMENTATION

| [Importing a Device Template | 341](#)

Importing a Device Template

IN THIS SECTION

- [Creating a Device Template File | 342](#)
- [Importing a Device Template File | 342](#)

Use the Device Templates page (**Resources > Templates > Device Templates**) to import a device template in JSON format for the customer.

NOTE: You must create a device template file before you can import a device template

Creating a Device Template File

To create a file of device information:

1. Select **Resources > Templates > Device Templates > Import Device Template**.

The Import Device Template page appears.

2. Click the **Download Sample JSON** link to open and save the sample JSON data file.

The sample file opens at the bottom of the page.

3. Save the template file with an appropriate name to your computer.

NOTE: You must retain the file format as .json to successfully upload the device template details to the Administration Portal.

4. Customize the sample JSON file according to the deployment.

5. Save the customized file.

Importing a Device Template File

Device templates are used to configure devices on a tenant site and these templates must be assigned to the device before you activate the device.

NOTE: A device template data file is required before your import device templates.

To import device template configuration:

1. Select **Resources > Templates > Device Templates > Import Device Template**.

The Import Device Template page appears.

2. Click **Browse** and navigate to the directory containing the device template configuration JSON file.

3. Select the file and click **Open**.

4. Click **Import Device Templates**. If you want to discard the import process, click **Cancel** instead.

The Device Templates Import Completed page appears with the details of the successful import.

5. Click **OK** to complete the import process.

The imported device template is displayed on the Device Template page.

Updating Stage-2 Configuration Template in a Device Template

Each device template has a set of configuration templates that can be used to deploy additional configuration on to the CPE device after it is activated. These templates are known as stage-2 configuration templates. You can add or remove stage-2 configuration templates from a device template.

NOTE: By default, the CPE device configuration is not supported on the CPE device. If you need the CPE device configuration, then you must configure it through stage-2 configuration in the device templates.

To add a stage-2 configuration template:

1. Select **Resources > Templates > Device Template**.

The Device Templates page appears.

2. Select a device template for which you want to add the stage-2 configuration and select **Edit Device Template > Stage-2 Config Templates**.

The Stage-2 Configuration Templates page appears. [Table 77 on page 344](#) lists the fields (and their descriptions) on the Stage-2 Configuration Templates page.

3. Click the add icon (+) and complete the configuration settings according to the guidelines provided in [Table 78 on page 345](#).

4. Click **Save**.

The new stage-2 configuration template is included in the device template.

Table 77: Fields on the Stage-2 Configuration Templates Page

Name	Description
Name	View the name of the stage-2 configuration template. Example: LAN side config
Component Name	View the name of the component through which the settings are configured. The components that are currently supported are: <ul style="list-style-type: none"> • JUNOS—Supported only on SRX Series Services Gateway. • Juniper Device Manager (JDM)—Supported on NFX250 device. JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—Supported on NFX250 device. JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—Supported on NFX250 device. vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor, providing perimeter security, IPsec connectivity, and filtering for malicious traffic without sacrificing reliability, visibility, or policy control. This virtual security and routing appliance ensures reliability and high availability for each application. Example: JUNOS
Hide	Displays whether the template is hidden on Customer Portal. <ul style="list-style-type: none"> • true—Template is not visible on Customer Portal. • false—Template is visible on Customer Portal. Example: false
Copy input from	Displays the template from which you copied the settings.
Auto Deploy	Displays whether the stage-2 configuration is automatically pushed to the device during ZTP process.

Table 77: Fields on the Stage-2 Configuration Templates Page (*continued*)

Name	Description
Enable for	Displays whether the stage-2 configuration template is enabled for all tenants, no tenants, or specific tenants.

Table 78: Fields on the Add New Template Page

Name	Description
Template	<p>Select the configuration template from the drop-down list. The configuration templates are designed in the Configuration Designer tool.</p> <p>Example: srx-basic-sdwan-cpe-config</p>
Display Name	<p>Specify the name of the template that you want to display on the configuration interface.</p> <p>Example: SDWAN Config</p>
Component Name	<p>Specify the component name through which the settings are configured. The components that are currently supported are:</p> <ul style="list-style-type: none"> • JUNOS—Supported on SRX Series Services Gateway. • Juniper Device Manager (JDM)— Supported on NFX250 device. JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—Supported on NFX250 device. JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—Supported on NFX250 device. vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor, providing perimeter security, IPsec connectivity, and filtering for malicious traffic without sacrificing reliability, visibility, or policy control. This virtual security and routing appliance ensures reliability and high availability for each application. <p>Example: JUNOS</p>
Hide	<p>Specify whether you want to hide the configuration template on Customer Portal. You might want to choose to hide the template if you are reusing the template for multiple components.</p> <ul style="list-style-type: none"> • hide—White dot on right with blue background. • show—White dot on left with gray background. <p>Example: hide</p>

Table 78: Fields on the Add New Template Page (*continued*)

Name	Description
Copy From Template	<p>If you have chosen to hide the configuration template on the user interface, then specify the template from which you want to copy the settings.</p> <p>Example: srx-mis-lan-to-wan-config</p>
Auto Deploy	<p>Specify whether the stage-2 configuration must be automatically pushed to the device during ZTP process. The available options are</p> <ul style="list-style-type: none"> • Same as global settings • Yes • No
Enabled for	<p>You can enable the stage-2 configuration template for all tenants, specific tenants, an SP administrator or an OpCo administrator.</p> <p>NOTE: Only users with SP administrator or OpCo administrator role can enable stage-2 configuration templates.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • All Tenants—Select this option to enable stage-2 configuration template for all tenants. Both SP and OpCo administrators can view templates for all tenants by switching the scope to the specific tenant. By default, stage-2 configuration templates assigned to all tenants are automatically applied to any new tenant. • No Tenants—Select this option to enable stage-2 configuration template for an SP administrator or an OpCo administrator. An SP administrator can modify the stage-2 configuration template. An OpCo administrator cannot modify the stage-2 configuration template. However, an OpCo administrator can clone the stage-2 configuration template and then modify the template. • Selective Tenants—Select this option to enable stage-2 configuration template for specific tenants. A tenant administrator can view and manage stage-2 template for a specific tenant. <p>When you select the Selective Tenants option, the Tenants section is displayed. Select one or more tenants. Click the greater-than icon (>) to move the selected tenant or tenants from the Available column to the Selected column. You can use the search icon on the top right of each column to search for tenant names.</p> <p>The default option is All Tenants.</p>

To remove a stage-2 configuration template:

1. Select **Resources > Templates > Device Templates**.

The Device Templates page appears.

2. Select the device template for which you want to remove the stage-2 configuration and then select **Edit Device Template > Stage-2 Config Templates**.

The Stage-2 Config Templates page appears.

3. Select a configuration template and click the delete icon (X).

A page requesting confirmation for the deletion appears.

4. Click **Yes** to confirm that you want to delete the stage-2 configuration template.

The configuration template is deleted.

RELATED DOCUMENTATION

| [About the Device Template Page](#) | 337

Configuring Stage-2 Initial Configuration in a Device Template

In general, the tenant administrators initiate stage-2 configuration through Customer Portal. However, in certain cases, the same stage-2 configuration needs to be deployed to CPE devices in all sites that are activated using a specific device template. In such cases, you can attach an initial configuration to a stage-2 configuration template of a device template. When a new CPE device in the site is activated using the device template, the initial configuration is automatically deployed to the CPE device.

The list of initial configurations that are supported are:

- Policies configuration
- LAN configuration
- SD-WAN configuration
- Routing configuration
- APN configuration

To update an initial configuration for stage-2 configuration template:

1. Select **Resources > Templates > Device Templates**.

The Device Templates page appears.

2. Select the device template for which you want to configure the stage-2 configuration and then select **Edit Device Template > Stage-2 Initial Config**.

The Stage-2 Initial Configuration page appears, listing the existing settings.

3. Complete the configuration settings according to the guidelines provided in [Table 79 on page 348](#), [Table 80 on page 349](#), and [Table 81 on page 349](#) and [Table 82 on page 350](#).

4. Click **Ok**.

Table 79: Fields for the VLAN Settings on the Stage-2 Initial Configuration Page

Field	Description
VLAN ID	Specify the identifier for the Layer 2 VLAN for the CPE device. Example: 230
IRB IP Prefix	Specify the IP address, including the subnet prefix, and the integrated routing and bridging (IRB) interface on the CPE device. Example: 192.0.2.15/24

Table 79: Fields for the VLAN Settings on the Stage-2 Initial Configuration Page (*continued*)

Field	Description
LAN Ports	Specify the LAN ports on the CPE device. Example: ge-0/0/0

Table 80: Fields for the LAN Settings on the Stage-2 Initial Configuration Page

Field	Description
LAN port	Specify the LAN ports on the CPE device. Example: ge-0/0/0
IP Address	Specify the IP address on the CPE device. Example: 192.0.2.255

Table 81: Fields for the SRX Basic SD-WAN Settings on the Stage-2 Initial Configuration Page

Field	Description
Manage App Group	Click to manage the application groups. The application group is predefined in the system for all SRX Series and vSRX configuration settings. The settings are preloaded and displayed on the portal. You can also create new application groups.
Manage App SLA Profile	Click to manage the application service-level agreements (SLA) profiles.
Rule Name	Specify the rule name. Example: critical-apps
Application/Groups	Specify the applications or application groups for the rule. Example: Oracle, SAP
Application SLA Profile	Specify the application SLA profile for the rule. Example: critical-apps

Table 82: Fields for the APN Configuration Settings on the Stage-2 Initial Configuration Page

Field	Description
Use default APN settings	<p>Click the toggle button to change the default APN settings.</p> <ul style="list-style-type: none"> • Enabled—Select this option to use the default APN setting that is shipped along with the CPE device. This is the default option. • Disabled—Select this option to configure the APN settings.
APN Settings	
APN Name	Enter the access point name (APN) of the gateway router.
SIM Change Required	<p>Click the toggle button to change the SIM card. You change the SIM card either to use a different LTE service provider or to use a private APN with the current LTE service provider.</p> <ul style="list-style-type: none"> • Enabled—Select this option to change the APN settings and to use a new SIM card. This is the default option. • Disabled—Select this option to change the APN settings without changing the SIM card.
Authentication Method	<p>Select the authentication method for the APN configuration.</p> <ul style="list-style-type: none"> • PAP— Select to use Password Authentication Protocol (PAP) authentication. This is the default option. • CHAP— Select to use Challenge Handshake Authentication Protocol (CHAP) authentication. • None—Select to indicate that there is no authentication method.
Authentication Information	
SIP User ID	Enter the Session Initiation Protocol (SIP) user ID for authentication.
SIP Password	Enter the SIP password for authentication.

RELATED DOCUMENTATION

[About the Device Template Page](#) | 337

Managing Configuration Templates

IN THIS CHAPTER

- [Configuration Templates Overview | 351](#)
- [Configuration Templates Workflow | 353](#)
- [About the Configuration Templates Page | 354](#)
- [Predefined Configuration Templates | 357](#)
- [Edit, Clone, and Delete Configuration Templates | 361](#)
- [Deploy Configuration Templates to Devices | 363](#)
- [Undeploy a Configuration Template from a Device | 369](#)
- [Dissociate a Configuration Template from a Device | 371](#)
- [Preview and Render Configuration Templates | 371](#)
- [Import Configuration Templates | 373](#)
- [Export a Configuration Template | 375](#)
- [Assign Configuration Templates to Device Templates | 376](#)
- [Add Configuration Templates | 378](#)
- [Jinja Syntax and Examples for Configuration Templates | 387](#)
- [View the Configuration Deployed on Devices | 399](#)

Configuration Templates Overview

Contrail Service Orchestration (CSO) offers a fully automated, end-to-end provisioning of customer premises equipment (CPE) devices. CSO utilizes configuration templates to provision parameters to enable the onboarding and configuration of Juniper Networks devices throughout the device lifecycle. Configuration templates (referred to as stage-2 templates in releases before CSO Release 5.1.0) also enable you to deploy customized configurations on devices that are managed by CSO. In short, configuration templates enable you to make configuration changes to Juniper devices by using the CSO GUI.

Configuration changes can be of two types:

- Global, which refers to configurations are common to all devices; for example, syslog or SNMP settings.
- Device-specific, which refers to configurations are unique for each device; for example, BGP configuration.

You can use configuration templates to push global (common) configurations to all devices or to specific devices.

By default, CSO provides predefined configuration templates that are pre-assigned to device templates. You can also create your own templates by importing a template, cloning a template and modifying its settings, or adding a template. Templates can be created by users with different roles. The availability of the templates is determined by the role of the user who created the template:

- Templates created by the SP Administrator (CSO on-premises version) users, are available to operating companies (OpCos), the OpCo's tenants, and the SP Administrator's tenants.
- Templates created by the OpCo Administrator users are available only to the OpCo and the OpCo's tenants.
- Templates created by the Tenant Administrator users are available only to the tenant.

You can either attach (assign) a configuration template to a device template, which enables the configuration to be deployed on devices which use that device template, or you can deploy a configuration template directly on a device.

TIP: In CSO, you may encounter the terms stage-1 and stage-2 configuration, which refer to the following:

- Stage-1 configuration is the initial configuration (pushed to the device) that allows CSO basic connectivity to a device.
- Stage-2 configuration is the configuration that CSO pushes to the device *after* the device connects with CSO.

Benefits

- Configuration templates provide a mechanism to create customized configurations and push the configurations to one or more devices, which enables you to deploy configurations beyond the standard configuration templates provided in CSO.

RELATED DOCUMENTATION

[Configuration Templates Workflow](#) | 353

Configuration Templates Workflow

Read the [“Configuration Templates Overview” on page 351](#) topic to gain a basic understanding of configuration templates.

In Customer Portal, users with the Tenant Administrator role can perform the configuration template workflow tasks indicated in this topic.

The high-level workflow for configuration templates is as follows:

1. You can use a pre-existing template (skip to step 2) or create a new template using one of the following methods:
 - Import a configuration template by specifying the template configuration file (Jinja syntax), Yang model file, and the Viewdef file. For more information, see [“Import Configuration Templates” on page 373](#).
 - Clone an existing configuration template and modify the cloned template. For more information, see [“Edit, Clone, and Delete Configuration Templates” on page 361](#).
 - Add a configuration template by specifying the template configuration and logic. For more information, see [“Add Configuration Templates” on page 378](#).
2. (Optional) Although this is an optional step, we recommend that you validate the configuration template by using the preview workflow *before* attaching the configuration template to a device template or deploying the configuration template directly on a device. For more information, see [“Preview and Render Configuration Templates” on page 371](#).
3. You can assign a configuration template to a device template from the Configuration Templates or the Device Templates pages. This enables you to deploy additional configuration on the device during zero touch provisioning (ZTP) and after the device is activated. For more information, see [“Assign Configuration Templates to Device Templates” on page 376](#) and [“Updating Stage-2 Configuration Template in a Device Template” on page 343](#).
4. You can deploy a configuration template directly on one or more devices that were previously activated, which enables you to deploy templates that were added after a device was activated or to deploy additional configuration to devices. You can deploy configuration templates to devices from the Configuration Templates or Tenant Devices pages. For more information, see [“Deploy Configuration Templates to Devices” on page 363](#).
5. (Optional) Dissociate or undeploy configuration templates:
 - You can dissociate a configuration template from a device, which remove the references to the configuration template from the device, but retains the configuration already deployed on the device. For more information, see [“Dissociate a Configuration Template from a Device” on page 371](#).

- You can undeploy the configuration template, which deletes the configuration previously deployed on the device, but retains the references to the configuration template. For more information, see [“Undeploy a Configuration Template from a Device” on page 369](#).

RELATED DOCUMENTATION

[About the Configuration Templates Page | 354](#)

[Jinja Syntax and Examples for Configuration Templates | 387](#)

About the Configuration Templates Page

IN THIS SECTION

- [Tasks You Can Perform | 354](#)
- [Field Descriptions | 355](#)

To access this page, click **Resources > Templates > Configuration Templates** in Customer Portal.

You can use the Configuration Templates page to view and manage configuration templates.

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

Tasks You Can Perform

In Customer Portal, users with the Tenant Administrator role can perform the following tasks from this page, while users with operator roles only have read capabilities.

- Clone a configuration template—[“Edit, Clone, and Delete Configuration Templates” on page 361](#).
- Deploy a configuration template on one or more devices—See [“Deploy Configuration Templates to Devices” on page 363](#).
- Preview and render a configuration template—See [“Preview and Render Configuration Templates” on page 371](#).

- View the details a configuration template—Select a configuration template and click **More > Template Details** or mouse over the configuration template click the Detailed View icon. The Detail for *Template-Name* pane appears on the right side of the page. See [Table 84 on page 356](#) for an explanation of the fields.
- Import a configuration template—See [“Import Configuration Templates” on page 373](#).
- Export a configuration template—[“Export a Configuration Template” on page 375](#).
- Assign a configuration template to a device template—See [“Assign Configuration Templates to Device Templates” on page 376](#).
- Add a configuration template—See [“Add Configuration Templates” on page 378](#).
- Edit or delete configuration templates—See [“Edit, Clone, and Delete Configuration Templates” on page 361](#).
- View the configuration deployed on one or more devices—See [“View the Configuration Deployed on Devices” on page 399](#).
- Search for configuration templates by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Sort configuration templates—Click a column name to sort the configuration templates based on the column name.

NOTE: Sorting and filtering is applicable only to some fields.

- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the Configuration Templates page.

Field Descriptions

[Table 83 on page 355](#) displays the description of the fields on the Configuration Templates page and [Table 84 on page 356](#) displays the description of the fields on the Detail for *Template-Name* Pane.

Table 83: Fields on the Configuration Templates Page

Field	Description
Name	Name of the configuration template.
Family	Device family to which the configuration template belongs.
Description	Description of the configuration template.

Table 83: Fields on the Configuration Templates Page (*continued*)

Field	Description
Deployed Devices	<p>Number of devices on which the configuration template was deployed. If the configuration template is not yet deployed on any devices then a blank cell is displayed.</p> <p>Click the <i>number-of-devices</i> link to view the configuration (for that configuration template) deployed on devices. See “View the Configuration Deployed on Devices” on page 399.</p>
Last Updated	Date and time on which the template was last updated.
Owner	<p>Depending on who added the configuration template, displays the following</p> <ul style="list-style-type: none"> • System—If the template is predefined or added by the Service Provider administrator • Tenant-Name—Name of the tenant if the template was added by an tenant administrator.

Table 84: Fields on the Detail for <Template-Name> Pane

Field	Description
<i>General tab</i>	
Name	See Table 83 on page 355 .
Description	See Table 83 on page 355 .
Family	See Table 83 on page 355 .
Format	<p>Format used by the configuration template:</p> <ul style="list-style-type: none"> • CLI • XML (Extensible Markup Language)
<i>Details tab</i>	<p>NOTE: If you want to add a new configuration template based on an existing one, you can copy the three files from the Details tab, modify the files as needed, and use the Import Configuration Template page to import a new template.</p>
Jinja Template	Displays the configuration in Jinja Template language syntax.
Data Model	Displays the Yang data model (configuration schema).
View Def	Displays the View Def (GUI configuration).

RELATED DOCUMENTATION

Predefined Configuration Templates

Contrail Service Orchestration (CSO) provides predefined configuration templates that you can access from the Configuration Templates page (**Resources > Configuration Templates**).

Predefined configuration templates are available for SRX Series, NFX150, and NFX250 devices:

- [Table 85 on page 357](#) lists the predefined configuration templates for SRX Series and NFX Series (NFX150 and NFX250) devices.
- [Table 86 on page 359](#) lists the predefined configuration templates for SRX Series devices.
- [Table 87 on page 359](#) lists the predefined configuration templates for NFX150 devices.
- [Table 88 on page 360](#) lists the predefined configuration templates for NFX250 devices.

Table 85: Predefined Configuration Templates for SRX Series and NFX Series (NFX150 and NFX250) Devices

Name	Description
common-banner	Configure the banner that appears when you log in to an SRX or NFX Series device.
common-disable-auto-negotiation	<p>Disable Ethernet autonegotiation on the interfaces of an SRX or NFX Series device.</p> <p>If you disable Ethernet autonegotiation, you must configure values for link mode and link speed when you deploy the template.</p>
common-dns	Configure Domain Name System (DNS) server settings on an SRX or NFX Series device.
common-firewall-filters	Configure firewall filters that determine whether to allow or deny traffic before it enters or exits a port to which the firewall filter is applied.
common-idp-sensor-packet-log	Configure an SRX or NFX Series device for packet capture, by defining the amount of memory to be allocated for packet capture and the maximum number of sessions that can generate packet capture data for the device at a time.
common-lacp	Configure link aggregation control protocol (LACP) on an SRX or NFX Series device.
common-local-user	Configure a local user on an SRX or NFX Series device.

Table 85: Predefined Configuration Templates for SRX Series and NFX Series (NFX150 and NFX250) Devices (*continued*)

Name	Description
common-nat-global-settings	Configure network address translation (NAT) settings (such as pool utilization alarms, port randomization, and so on) on an SRX or NFX Series device.
common-ntp	Configure Network Time Protocol (NTP) settings on an SRX or NFX Series device.
common-password-config	Change the default password for a root user on an SRX or NFX Series device.
common-pre-id-default-policy	<p>Configure the default policy action that occurs prior to dynamic application identification (AppID).</p> <p>During the initial policy lookup phase, which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list, an SRX or NFX Series device applies the default security policy until a more explicit match is found.</p>
common-sdwan-dhcprelay	Configure extended DHCP relay and DHCPv6 relay options on an SRX or NFX Series device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP Request and DHCP Reply packets between a DHCP client and a DHCP server.
common-service	Configure the FTP, SSH, and NETCONF settings on an SRX or NFX Series device.
common-snmp-config-basic	Configure basic SNMP version 2 (SNMPv2) parameters on an SRX or NFX Series device.
common-static-routes	<p>Configure static routes to be installed in the routing table for an SRX or NFX Series device.</p> <p>You can specify one or more routes within a single static statement, and you can specify one or more static options in the configuration.</p> <p>For more information, see static (Routing Options).</p>
common-syslog	Configure syslog settings on an SRX or NFX Series device.
common-UTM-global	Configure the routing instance, on an SRX or NFX Series device, through which the DNS server can be reached to resolve the unified threat management (UTM) Web filtering URL.

Table 86: Predefined Configuration Templates for SRX Series Devices

Name	Description
ngfw-ipsec-vpn	Configure IPsec VPN settings for an SRX next-generation firewall (NGFW) device.
srx-dhcp	Configure an SRX Series device as a Dynamic Host Configuration Protocol (DHCP) server.
srx-dns	Configure Domain Name System (DNS) server settings on an SRX Series device.
srx-hub-breakout-stage2-config	<p>Use this template to configure NAT on WAN links of provider hubs for breakout traffic. You can configure NAT on provider hubs with DATA_ONLY and OAM_AND_DATA capabilities.</p> <p>The configuration template can be applied per tenant provided, the tenant has at least one branch site connected to the provider hub configured for NAT.</p> <p>NOTE: You can configure NAT using the template only on existing WAN links and not on additional WAN links later added by tenants.</p> <p>Interface-based source NAT is used as the tunnel in the NAT configuration template.</p>
srx-sdwan-dhcp-relay	Configure extended DHCP relay and DHCPv6 relay options on an SRX Series device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP Request and DHCP Reply packets between a DHCP client and a DHCP server.
srx-sdwan-mgmt	<p>Configure the SNMP version 3 (SNMPv3), NTP, syslog, and TACACS parameters for managing an SRX Series device.</p> <p>For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the Allow TACACS Access and Allow SNMP Access toggle buttons in the associated device template.</p>
srx-vrrp	Configure virtual router redundancy protocol (VRRP) on an SRX Series device.

Table 87: Predefined Configuration Templates for NFX150 Devices

Name	Description
nfx3-sdwan-mgmt	<p>Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing an NFX150 device.</p> <p>For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the Allow TACACS Access and Allow SNMP Access toggle buttons in the associated device template.</p>

Table 88: Predefined Configuration Templates for NFX250 Devices

Name	Description
nfx-cluster-sdwan-gwr-dhcprelay	Configure extended DHCP relay and DHCPv6 relay options on an NFX250 cluster and enable the cluster to function as a DHCP relay agent. A DHCP relay agent forwards DHCP Request and DHCP Reply packets between a DHCP client and a DHCP server.
nfx-sdwan-gwr-mgmnt	<p>Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing the gateway router (vSRX) on an NFX250 device.</p> <p>For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the Allow TACACS Access and Allow SNMP Access toggle buttons in the associated device template.</p>
nfx-sdwan-jcp-mgmnt	<p>Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing the Junos Control Plane (JCP) component of an NFX250 device.</p> <p>For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the Allow TACACS Access and Allow SNMP Access toggle buttons in the associated device template.</p>
nfx-sdwan-jdm-mgmnt	<p>Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing the Juniper Device Manager (JDM) component of an NFX250 device.</p> <p>For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the Allow TACACS Access and Allow SNMP Access toggle buttons in the associated device template.</p>

RELATED DOCUMENTATION

[About the Configuration Templates Page](#) | 354

Edit, Clone, and Delete Configuration Templates

IN THIS SECTION

- [Edit a Configuration Template | 361](#)
- [Clone a Configuration Template | 362](#)
- [Delete a Configuration Template | 363](#)

Users with the Tenant Administrator role can modify the parameters of existing configuration templates, clone existing configuration templates, and delete configuration templates that are no longer being used.

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

Edit a Configuration Template

Users with the Tenant Administrator role can edit only the templates that they added (created).

To modify a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to modify and click the edit (pencil) icon.

The Edit Configuration Template page appears. The fields on this page are same as the fields that you configure in the Add Configuration Template workflow.

3. Modify the fields as needed.

Refer to [“Add Configuration Templates” on page 378](#) for an explanation of the fields.

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The modifications are saved and you are returned to the Configuration Templates page, where a confirmation message is displayed. If the configuration template was previously deployed on a device or assigned to a device template, then you must redeploy the configuration template for the changes to take effect.

Clone a Configuration Template

To clone a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to clone and click **Clone**.

- If you select a configuration template that was added in CSO Release 5.3.0, the Clone Configuration Template page appears. Proceed to Step 3.
- If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.

- a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

- b. Select the template again and click **Clone**.

The Clone Configuration Template page appears.

3. In the **Template Name** field, enter a unique template name that can only contain alphanumeric characters and hyphens up to a maximum of 64 characters.
4. Click **OK**.

You are returned to the Configuration Templates page and a confirmation message appears at the top of the page indicating the status of the clone operation.

After a template is cloned successfully, you can modify the template if needed. See the preceding section for details.

Delete a Configuration Template

To delete a configuration template:

NOTE:

- You cannot delete predefined configuration templates.
- You can delete a configuration template only if the following conditions hold good:
 - You added (created) the template.
 - The template is not assigned to a device template.
 - The template is not deployed on a device.

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to delete and click the **X** (delete) icon.

You are asked to confirm the delete operation.

3. Click **Yes**.

You are returned to the Configuration Templates page and a popup appears indicating whether the deletion was successful or not.

RELATED DOCUMENTATION

| [Preview and Render Configuration Templates](#) | 371

Deploy Configuration Templates to Devices

IN THIS SECTION

- [Deploy from the Configuration Templates Page](#) | 364
- [Deploy from the Devices Page](#) | 368

In Customer Portal, users with the Tenant Administrator role can deploy a configuration template directly on one or more devices that were previously activated. This enables you to deploy configuration templates added after a device was activated or to deploy additional configuration to devices.

You can deploy configuration templates to devices from the Configuration Templates or the Devices pages.

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

Deploy from the Configuration Templates Page

To deploy a configuration template to one or more devices:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want deploy and click **Deploy to Devices**.

- If you select a configuration template that was added in CSO Release 5.3.0, the Deploy Template *Template-Name* To Devices page appears. Proceed to Step 3.
- If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.
 - a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

- b. Select the template again and click **Deploy to Devices**.

The Deploy Template *Template-Name* To Devices page appears.

3. Complete the configuration according to the guidelines provided in [Table 89 on page 365](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The settings that you entered are saved and you are returned to the Configuration Templates page. A confirmation message appears indicating that a job was created. For each device, a separate job is triggered to deploy the configuration.

You can view the status of the jobs from the Jobs page (**Monitor > Jobs**).

Table 89: Deploy Template <Template-Name> To Devices Settings

Setting	Guideline
Select Devices	
Configuration Template	Displays the name of the configuration template that you are deploying; you cannot modify this field.
Component Name	<p>This field is displayed only for NFX250 devices.</p> <p>Select the component of the NFX250 device on which to deploy the template:</p> <ul style="list-style-type: none">• JCP—Junos Control Plane• JDM—Junos Device Manager• GWR-Gateway Router

Table 89: Deploy Template <Template-Name> To Devices Settings (*continued*)

Setting	Guideline
Devices	<p>You can specify the devices on which you want to deploy the configuration template in the following ways:</p> <ul style="list-style-type: none"> By adding the devices manually: <ol style="list-style-type: none"> From the list of devices displayed, select one or more devices by clicking the check box next to each device name. <p>NOTE: You can search for devices or filter the list of devices displayed.</p> By uploading a comma-separated values (CSV) file containing the device information: <p>NOTE: You must ensure that the CSV file is in the format that CSO can read and that the number of device records is 200 or lower. You can download a sample file by clicking the Download Sample CSV File button.</p> <ol style="list-style-type: none"> Click Upload CSV File. <p>The Upload CSV File page appears.</p> <ol style="list-style-type: none"> Click Browse to open the file selection dialog, select a file, and click Open. <p>The name of the file that you selected is displayed in the CSV File field.</p> <ol style="list-style-type: none"> Click OK. <p>You are returned to the previous page where the devices that you imported are selected and displayed in the table.</p> <p>Click Next.</p> <p>You are taken to the Configure Global Parameters or the Configure Device Parameters tab.</p>
<i>Configure Global Parameters</i>	<p>NOTE: This tab is displayed only if the configuration template contains parameters that are global in scope.</p> <p>Specify the global parameters that are common to all the devices that you selected in the preceding step. After you are done, click Next.</p> <p>You are taken to the Configure Device Parameters tab.</p>
<i>Configure Device Parameters</i>	

Table 89: Deploy Template <Template-Name> To Devices Settings (*continued*)

Setting	Guideline
Devices	<p>The devices that you selected in the preceding step are displayed in the Devices table, and the first device is selected by default.</p> <p>For each device, the device name, device family, operational status, and the configuration status are displayed. When you first arrive on this tab, the configuration status for each device is <i>Not configured</i>.</p> <p>The <i>Device-Name</i> Parameters pane on the right displays the input parameters (from the configuration template) that you can specify for each device.</p> <p>After you specify the values for one device, you can select a different device and enter the configuration values.</p> <ul style="list-style-type: none"> • If the configuration template contains validations for the parameters, CSO validates the values you entered for the device and changes the configuration status to Valid and displays a green check mark (✓). • If the configuration template does not contain any validations, CSO changes the configuration status to Valid and displays a green check mark (✓). • If the values that you entered do not match the validation, the configuration status displays Invalid. <p>NOTE: You can optionally delete a device by selecting the device and clicking the delete (trash can) icon.</p> <p>After you specify the input parameter values for all the devices and ensure that the configuration status of all devices is Valid, click Next.</p> <p>You are taken to the Summary tab.</p>
Summary	
Devices	<p>The devices that you selected in the preceding step are displayed in the Devices table, and the first device is selected by default.</p> <p>For each device, the device name, device family, and operational status are displayed.</p> <p>For each device, the <i>Device-Name</i> Configuration pane on the right displays the actual configuration that will be deployed on the device.</p> <p>After you review the configuration for all the devices, click Next.</p> <p>You are taken to the Deploy tab.</p>
Deploy	

Table 89: Deploy Template <Template-Name> To Devices Settings (*continued*)

Setting	Guideline
Deployment Schedule	<p>Specify whether the configuration should be deployed on devices immediately(Deploy now) or deployed later (Deploy later).</p> <p>If you choose to deploy the configuration later, you must enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the deployment to occur.</p>

Deploy from the Devices Page

To deploy a configuration template to one or more devices:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select the device on which you want deploy and click **More > Deploy Configuration Template**.

NOTE: The devices that you select must belong to the same device family. If you select devices from different device families, CSO displays an error message.

The Deploy Template to Device *Device-Name* page appears.

3. From the **Configuration Templates** table, select the configuration template that you want to deploy and click **Next**.

The configuration templates displayed are filtered based on the device family of the devices that you selected.

- If you select a configuration template that was added in CSO Release 5.3.0, proceed to Step 4.
- If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.
 - a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

The template is automatically upgraded to CSO Release 5.3.0 and the Devices page appears.

- b. Select the device again and click **More > Deploy Configuration Template**.

The Deploy Template to Device *Device-Name* page appears.

4. The rest of the deploy workflow is the same as you encounter if you initiate the deployment from the Configuration Templates page. Complete the configuration according to the guidelines provided in [Table 89 on page 365](#)

NOTE: Fields marked with an asterisk (*) are mandatory.

5. Click **OK**.

The settings that you entered are saved and you are returned to the Devices page. A confirmation message appears indicating that a job was created. For each device, a separate job is triggered to deploy the configuration.

You can view the status of the jobs from the Jobs page (**Monitor > Jobs**).

RELATED DOCUMENTATION

| [Assign Configuration Templates to Device Templates](#) | 376

Undeploy a Configuration Template from a Device

As a tenant administrator, you can undeploy a configuration template when you no longer need the configuration deployed on the device.

Undeploying a configuration template removes the configuration pushed to the device when the configuration template was deployed.

To remove only the references to the configuration template without removing the configuration pushed to the device, you must dissociate the configuration template. See [“Dissociate a Configuration Template from a Device” on page 371](#) for details.

NOTE: You can undeploy configuration templates only from devices with Management Status **Provisioned**. In addition, the configuration templates must have been previously deployed (Deployment Status **Deployed**) on the device.

To undeploy a configuration template:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the *Device-name* link for the device.

The *Device-Name* page appears.

3. From the **Configuration Template** tab, select the configuration template that you want to undeploy and click **Undeploy**.

- If you select a configuration template that was added in CSO Release 5.3.0, an alert message appears, asking you to confirm the undeploy operation. Proceed to Step 4.
- If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to CSO Release 5.3.0. You must go through the Edit workflow to upgrade the version.
 - a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

- b. Select the template again and click **Undeploy**.

An alert message appears, asking you to confirm the undeploy operation.

4. Click **Yes**.

A message indicating that the undeploy configuration template job was triggered is displayed.

You can click the link in the message to view the progress of the job or view the progress on the Jobs page:

- If the job completes successfully, a confirmation message appears, indicating that the configuration template was undeployed from the device.
- If the job fails, an error message appears. You can repeat the procedure to undeploy the configuration template.

RELATED DOCUMENTATION

[Deploy Configuration Templates to Devices](#) | 363

Dissociate a Configuration Template from a Device

As a tenant administrator, you can dissociate a configuration template when you no longer want the template to be associated with your device. Dissociating a configuration template removes references to the configuration template from the device but does not remove the configuration pushed to the device.

To remove the configuration pushed to the device, you must undeploy the configuration template. See [“Undeploy a Configuration Template from a Device” on page 369](#) for details.

To dissociate a configuration template:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the **Device-Name** link for the device from which you want to dissociate the configuration template.

The **Device-Name** page appears.

3. From the **Configuration Template** tab, select the configuration template that you want to dissociate from the device and click **Dissociate**.

An alert message appears, asking you to confirm the dissociate operation.

4. Click **Yes**.

If the dissociation is successful, a confirmation message appears, indicating that the references to the configuration template were removed from the device.

If the dissociation fails, repeat the procedure to dissociate the configuration template.

Preview and Render Configuration Templates

In Customer Portal, users with the Tenant Administrator role can use the Preview workflow to validate a configuration template by entering values for the configuration template and then rendering the template to view the configuration.

Although this is not mandatory, we recommend that you use this workflow to validate a configuration template before attaching it to a device template or deploying it on a device.

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

To preview and render a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to check and click **Render Configuration**.

- If you select a configuration template that was added in CSO Release 5.3.0, the Preview Configuration page appears displaying the parameters configured for the template. Proceed to Step 3.
- If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.
 - a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

- b. Select the template again and click **Render Configuration**.

The Preview Configuration page appears displaying the parameters configured for the template.

3. Specify values for the parameters as needed.

NOTE: Fields marked with an asterisk (*) are mandatory.

4. After you have entered the necessary parameters, click **Render**.

The Rendered Config page appears displaying the configuration rendered based on the configuration template and the values that you specified.

5. Check if the configuration was rendered correctly.

If the configuration was not rendered correctly, you can modify the configuration template as needed. See [“Edit, Clone, and Delete Configuration Templates” on page 361](#).

6. Click **OK**.

You are returned to the Preview Configuration Template page.

7. Click **Cancel** to exit the Preview Configuration Template page.

You are returned to the Configuration Templates page. You can assign the configuration template to one or more device templates.

RELATED DOCUMENTATION

[Assign Configuration Templates to Device Templates](#) | 376

Import Configuration Templates

In Customer Portal, users with the Tenant Administrator role can import a configuration template by specifying the parameters using a configuration template file (Jinja template language), Yang model file (schema for the configuration), and the Viewdef file (configuration of the UI).

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

To import a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Select **More > Import**.

The Import Configuration Template page appears.

3. Complete the configuration according to the guidelines provided in [Table 90 on page 374](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the Configuration Templates page and a popup appears displaying the status of the import operation.

5. Click **OK** to close the popup.

You are returned to the Configuration Templates page.

If the configuration template is imported successfully, you can validate the configuration template by using the Preview workflow and then assign the configuration template to a device template or deploy it on a device.

Table 90: Import Configuration Template Settings

Setting	Guideline
Template Name	Enter a unique name that can only contain alphanumeric characters and hyphens; 64-character maximum.
Description	Enter a description for the configuration template.
Output Config Format	Select the output configuration format for the template: <ul style="list-style-type: none"> • CLI (default) • XML
Device Family	Select the device family for which you are adding the template; for example, juniper-nfx.
Configuration Template File	Specify the file containing the configuration (in Jinja Template language syntax) by clicking the Browse button to navigate to the directory where the configuration template file is located and selecting the file.
Yang Model File	Specify the Yang data model (configuration schema) file by clicking the Browse button to navigate to the directory where the Yang model file is located and selecting the file.
Viewdef File	Specify the Viewdef file, which contains the configuration for the UI, by clicking the Browse button to navigate to the directory where the Viewdef file is located and selecting the file.

RELATED DOCUMENTATION

[Preview and Render Configuration Templates | 371](#)

[Deploy Configuration Templates to Devices | 363](#)

Export a Configuration Template

As a tenant administrator, you can export a configuration template as a ZIP file if you want to modify the template offline and then import it as a new template.

The ZIP file contains the configuration template file (Jinja template language), Yang model file (schema for the configuration), and the Viewdef file (configuration of the UI).

To export a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Select a configuration template from the list and click **More > Export**.

- If you select a configuration template that was added in CSO Release 5.3.0, the configuration template is automatically downloaded as a ZIP file to your local file system.
- If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.

- a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

- b. Select the template again and click **Export**.

The configuration template is automatically downloaded as a ZIP file to your local file system.

You can modify the configuration template files as needed and import the files back into Customer Portal.

RELATED DOCUMENTATION

[About the Configuration Templates Page | 354](#)

[Import Configuration Templates | 373](#)

Assign Configuration Templates to Device Templates

In Customer Portal, users with the Tenant Administrator role can assign a configuration template to one or more device templates. Associating a configuration template with a device template enables you to deploy additional configuration on the device during ZTP and after the device is activated.

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

To assign a configuration template to one or more device templates:

1. Select **Resources > Templates > Configuration Templates**.
The Configuration Templates page appears.
2. Select the configuration template that you want to assign and select **More > Assign to Device Template**.
The Assign Configuration Template to Device Templates page appears.
3. Complete the configuration according to the guidelines provided in [Table 91 on page 376](#)

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.
You are returned to the Configuration Templates page and a popup appears indicating whether the assignment is successful or has failed. If the assignment failed, you can retry the assignment or contact Juniper Networks support.

If the assignment is successful, the configuration parameters are displayed in the *Device-Name* page and you can enter values for the configuration and deploy the changes on the device.

Table 91: Assign Configuration Template to Device Template Settings

Setting	Guideline
Template Settings	
Template	Displays the name of the configuration template that you are assigning; you cannot modify this field.

Table 91: Assign Configuration Template to Device Template Settings (*continued*)

Setting	Guideline
Display Name	Enter the name that you want displayed on the <i>Device-Name</i> page.
Component Name	<p>For NFX250 devices, select the component name to which the configuration should be deployed. The components that are currently supported are:</p> <ul style="list-style-type: none"> • Juniper Device Manager (JDM)—JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor.
Auto Deploy	<p>Specify whether the configuration should be deployed automatically on the device during the zero touch provisioning (ZTP) process. The options are:</p> <ul style="list-style-type: none"> • Yes—Deploy the configuration automatically on the device during ZTP. • No (Default)—Don't deploy the configuration is not deployed automatically on the device during ZTP. • Same as global settings—Use the same settings as the one configured in the device template.
<i>Device Templates</i>	
Select Device Templates	<p>The list of device templates to which you can assign the configuration template are displayed in a grid along with some information about the template. CSO displays only those device templates whose device family matches the device family of the configuration template.</p> <p>Select one or more device templates to which you want to assign the configuration template.</p>

RELATED DOCUMENTATION

[Deploy Configuration Templates to Devices](#) | 363

Add Configuration Templates

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

In Customer Portal, users with the Tenant Administrator role can add a configuration template by providing the device configuration in the Jinja template language syntax.

NOTE:

- Before you add the configuration template, ensure that you have the device configuration ready.
- We recommend that you use a working device configuration to add the configuration template.

To add a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Click the + (add) icon.

The Add Configuration Template page (wizard) appears.

NOTE: Fields marked with an asterisk (*) are mandatory.

3. Configure the fields on the Basic Information tab according to the guidelines provided in [Table 92 on page 379](#).

Click **Next** to go to the Templatize Config tab.

4. Add the configuration on the Templatize Config tab. Refer to [Table 93 on page 379](#) for an explanation of the actions on this tab.

Click **Next** to go to the Generated UI tab, where the UI for the parameters that you entered is generated and displayed.

5. Perform one or more actions on this tab, as explained in [Table 94 on page 380](#).

6. Click **Save**.

The configuration template is added and you are returned to the Configuration Templates page, where a confirmation message is displayed. You can assign the configuration template to device templates or deploy the template on devices.

Table 92: Basic Information Settings (Add Configuration Template Page)

Setting	Guideline
Template Name	Enter a unique name that can only contain alphanumeric characters and hyphens; 64-character maximum.
Description	Enter a description for the configuration template.
Output Config Format	Select the output configuration format for the template: <ul style="list-style-type: none"> • CLI (default) • XML
Device Family	Select the device family for which you are adding the template; for example, juniper-nfx.
Can be re-deployed	Enable this toggle button if you want CSO to deploy the configuration template again when you redeploy the template. CSO deploys the template even if there are no configuration changes since the previous deployment. If this button is disabled, which is the default, then CSO does not deploy the template again if there are no changes since the previous deployment.
	Click Next to continue.

Table 93: Templatize Config Actions (Add Configuration Template Page)

Action	Description
View a sample configuration	You can view a sample configuration by clicking the Sample Configuration link near the top of the tab. The sample configuration appears in a new tab in your browser.
Add the device configuration	In the inline editor, copy and paste the device configuration ensuring that the syntax follows the Jinja Template language. CSO detects the template parameters corresponding to the configuration that you entered and displays them in the Parameters pane. For more information, see “Jinja Syntax and Examples for Configuration Templates” on page 387 .

Table 93: Templatize Config Actions (Add Configuration Template Page) (continued)

Action	Description
Advanced Mode	<ul style="list-style-type: none"> When advanced mode is disabled, which is the default, CSO converts the configuration that you entered in Jinja Template language to a Junos OS configuration that uses Junos OS configuration groups. (Configuration groups make it easier to configure and maintain Junos OS configurations; see Understanding Junos OS Configuration Groups.) CSO also automatically includes the commands to delete the configuration groups in the configuration template. If you trigger an undeploy configuration template workflow, CSO uses these commands to delete the configuration. Therefore, to avoid conflict with the commands that CSO automatically includes, ensure that you do not manually include commands related to configuration groups (as part of the device configuration). When advanced mode is enabled, CSO converts the configuration that you entered in Jinja Template language but does not use Junos OS configuration groups and does not include commands to delete the configuration. Therefore, if you plan to undeploy the configuration template later, you must ensure that you manually enter the commands to delete the configuration as part of the device configuration so that CSO can use these commands to delete the configuration.
[Detected Parameters]	<p>Check that the parameters detected match the configuration that you added to the template:</p> <ul style="list-style-type: none"> If the parameters detected do not match, check the Jinja syntax that you used for the template configuration and make any changes needed in the inline editor. If the parameters detected match the configuration that you added to the template, click Next to continue. <p>CSO validates the Jinja template syntax and displays an error message if there are any errors.</p>

Table 94: Generated UI Actions (Add Configuration Template Page)

Action	Description
Reorder the UI	Drag and drop individual fields, grids, or sections to change the order in which the parameters appear on the UI.

Table 94: Generated UI Actions (Add Configuration Template Page) (continued)

Action	Description
Modify the settings for a field, section, or grid	<p>To modify the settings for a field, section, or grid:</p> <ol style="list-style-type: none"> 1. Click the settings (gear) icon next to the field, section, or grid. The Parameter Settings pane appears on the right side of the page, displaying the Basic Settings and Advanced Settings tabs. 2. Modify the fields on these tabs, as needed. See Table 95 on page 381 for an explanation of the fields on these tabs. 3. Click Save Settings for each field to save your changes. The modifications that you made are displayed on the UI.
Reset the generated UI	Click Undo all Edits to discard the changes that you made and undo the changes made on the UI.
Preview configuration	<p>Previewing the configuration enables you to check the configuration template that you added.</p> <p>To preview a configuration template:</p> <ol style="list-style-type: none"> 1. Click Preview Configuration. The Preview Configuration page appears, displaying the configuration that was rendered based on the values that you entered. 2. Check if the configuration was rendered correctly. <ul style="list-style-type: none"> • If the configuration was not rendered correctly, click the close (X) icon to go back and make modifications as needed. • If the configuration was rendered correctly, click OK. <p>You are returned to the Generated UI page.</p>

Table 95: Parameter Settings (Add Configuration Template Page)

Setting	Guideline
<i>Basic Settings Tab</i>	Fields populated in this tab are based on the input type that you select.

Table 95: Parameter Settings (Add Configuration Template Page) (continued)

Setting	Guideline
Input Type	<p>Select the input type for the parameter in the configuration template:</p> <ul style="list-style-type: none"> • Text (default): If the input value for the parameter is a string of characters. • Number: If the input value for the parameter is a number. • E-mail: If the input value for the parameter is an e-mail address. • IPv4: If the input value for the parameter is an IPv4 address. • IPv4 Prefix: If the input value for the parameter is an IPv4 prefix. • IPv6: If the input value for the parameter is an IPv6 address. • IPv6 Prefix: If the input value for the parameter is an IPv6 prefix. • Toggle Button (Boolean): If the input value for the parameter is a boolean value (true or false). • Dropdown: If the input value for the parameter is selected from a list. • Password: If the input value for the parameter is a password. The value that you enter is masked (default). (Optional) Click the Show Password (eye) icon to unmask the password. • Confirm Password: If the input value for the parameter is to confirm the password. If you select this option, a Confirm Password field appears on the UI. The value that you enter is masked (default). (Optional) Click the Show Password (eye) icon to unmask the password.
Label	Enter the label that you want displayed (on the UI) for the parameter.
Default Value	Specify a default value for the parameter.
Validation Criteria	<p>For Text input type, select one or more validation criteria against which the input value will be checked.</p> <p>If the value that you entered for the parameter on the UI does not meet the selected validation criteria, an error message appears.</p>
Description	Enter an explanation for the parameter, which will appear when you hover over the Help (?) icon for the parameter; the maximum length allowed is 256 characters.
Global Scope	Click the toggle button to make the parameter common across all devices to which the configuration template is being deployed to. If you disable the toggle button, which is default, the parameter must be specified for each device.

Table 95: Parameter Settings (Add Configuration Template Page) (continued)

Setting	Guideline
Hidden	<p>Click the toggle button to hide the parameter on the UI when you preview and deploy the template.</p> <p>Typically, this option is used to hide a parameter and display it in the template only when an event is triggered. By default, the toggle button is disabled, which means that the parameter is displayed.</p>
Required	<p>Click the toggle button to make the parameter mandatory; parameters that are mandatory are marked with an asterisk (*) on the UI.</p>
Maximum Value	<p>For parameters that are numbers, enter the maximum value (up to 16 digits) for the input.</p>
Minimum Value	<p>For parameters that are numbers, enter the minimum value (up to 16 digits) for the input.</p>
Fields Visible (Toggle Disabled)	<p>For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is disabled (boolean value is FALSE).</p>
Fields Visible (Toggle Enabled)	<p>For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is enabled (boolean value is TRUE).</p>

Table 95: Parameter Settings (Add Configuration Template Page) (continued)

Resource Type	<p>For Dropdown input type, select the type of resource from which you want to retrieve data:</p> <ul style="list-style-type: none">• Static Resource—Resources in the list on the UI are mapped to the values that you specify.<ul style="list-style-type: none">• To add a static resource:<ol style="list-style-type: none">1. Click the + (add) icon.<p>Cells appear in the List Values table.</p>2. Click inside the cells to specify values for the Label (name for the option in the list), Value (value for the option in the list), and Visibility (conditional visibility based on the option selected from the list) fields.3. click ✓ (check mark) to save your changes.<p>The values that you specified are displayed in the List Values table.</p>• To edit a static resource, select the resource and click the edit (pencil) icon.• To delete a static resource, select the resource and click the X (delete) icon.• Dynamic Resource—Resources in the list on the UI are mapped to the predefined services in CSO.<p>Click the <i>Resource Management</i> link to view add, edit, and delete dynamic resources. The Manage Dynamic Resources page appears displaying the existing resources.</p><ul style="list-style-type: none">• To add a dynamic resource:<ol style="list-style-type: none">1. Click the + (add) icon.<p>The Add Dynamic Resource page appears.</p>2. Complete the configuration according to the guidelines specified in Table 96 on page 385. Fields marked with an asterisk (*) are mandatory.3. Click OK to save the resource.<p>You are returned to the Manage Dynamic Resources page, where the resource that you added appears.</p>4. Click OK.<p>You are returned to the Add Configuration Template page. The resource or resources that you added are available in the Resource list on the Parameter Settings pane.</p>• To edit a dynamic resource, select the resource and click the edit (pencil) icon.• To delete a dynamic resource, select the resource and click the X (delete) icon.
---------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 95: Parameter Settings (Add Configuration Template Page) (*continued*)

Key	<p>For data in a table, select a column from the dropdown list that is to be used as a key.</p> <p>The column that you select is marked as unique (Unique Key), indicating that the entries in this column must be unique.</p> <p>Keys are unique identifiers used in defining entries (in a table) in the Yang data hierarchy. They help distinguish entries in a column.</p>
<i>Advanced Settings Tab</i>	
Regex	<p>Enter a regular expression (regex pattern) to validate the input value.</p> <p>A regular expression defines a search pattern that is used to match characters in a string.</p> <p>For example, the regular expression [A-Z] matches the input with the characters A through Z.</p> <p>If the input consists of characters other than A through Z, an error message (as specified in the Invalid Message field) appears.</p>
Error Message (Regex)	Enter an error message that you want displayed on the UI when the input value does not match the specified regular expression.
Remote Validation	Enter a JavaScript function to validate the input value.
<i>Event List</i>	
Event Name	Select an event from the list based on which the parameter is conditionally displayed.
Event Handler	Enter a JavaScript function that specifies the actions that the event handler takes in response to an event.

Table 96: Fields on the Add Dynamic Resource Page

Field	Guideline
<i>Data Source</i>	
Name	Enter a unique name for the resource.
Source Type	<p>Select the source from which you want to retrieve data:</p> <ul style="list-style-type: none"> • Service based, which uses predefined services to retrieve data. • URL based, which uses a URL of the API to retrieve data.

Table 96: Fields on the Add Dynamic Resource Page (*continued*)

Field	Guideline
Service	For service-based source type, select a predefined service from which you want to retrieve data.
Entity	For service-based source type, select an entity for which you want to retrieve data.
URL	For URL-based source type, enter the URL of the API to be used for the request.
Method	For the URL-based source type, select the type of HTTPS method (GET or POST) to be used for the resource.
POST Body	For POST method, enter the format of the payload (in JavaScript Object Notation [JSON] format) of the API method, which is sent to the server.
Mock Result	Specify a mock result (in JSON format) if the API request is unable to retrieve data.
<i>Result Mapping</i>	
Result Mapping	<p>Select the type of processing to be done on the output of the remote request:</p> <ul style="list-style-type: none"> • Script—Use this option if you want to use a script (in JSON format) to process the output. • Mapping—Use this option if you want to map the output using a base path.
Mapping Script	To process the output by using a script, enter a mapping script in JSON format.
Base Path	To process the output by using a base path, enter the base path (JSONPath expression) of the variable in the output from which you want to extract the data; for example, interface.
Label Field	Select whether you want the names, UUIDs, or management status (for the selected entity) displayed as options in the list on the UI.

Table 96: Fields on the Add Dynamic Resource Page *(continued)*

Field	Guideline
Value Field	<p>Select a value (such as names, management status, and so on) that you want to associate with the labels (options) in the list on the UI.</p> <p>When you select an option from the list and save the configuration template, CSO processes its associated value (in the backend).</p>
Extra Fields	<p>Specify the additional values that you want to associate with the labels (options) in the list on the UI. When you select an option from the list on the UI, its associated additional value can be used to trigger an event, when a condition is met, by using a JavaScript function. You specify the JavaScript function in the Event Handler field.</p>

RELATED DOCUMENTATION

[Preview and Render Configuration Templates | 371](#)

Jinja Syntax and Examples for Configuration Templates

IN THIS SECTION

- [Jinja Syntax and CSO Keywords | 388](#)
- [Example 1: Convert a Single Junos OS Command to Jinja Syntax | 390](#)
- [Example 2: Convert a Junos OS Configuration Snippet to Jinja Syntax | 391](#)
- [Example 3: Use Conditional Logic | 393](#)
- [Example 4: Use Variable Substitution | 395](#)
- [Example 5: Use Filters, Concatenation, and Set Variables | 396](#)
- [Example 6: Test a Value | 397](#)

CSO configuration templates consist of three components:

- A Jinja template configuration, which contains the logic and the configuration for the configuration template. (Jinja is a template engine for Python and you can find several Jinja resources on the Web.)
- A Yang data model file, which contains the descriptors for the configuration schema.
- A ViewDef (view definition) file, which is a JavaScript Object Notation (JSON) file that is used to specify the GUI aspects of the configuration template.

When you use the Add Configuration Template workflow to add a template, you specify the template configuration and logic by using the Jinja template language. CSO then generates the Yang data model and the ViewDef files automatically based on template configuration and logic that you specified. The generation of the Yang and ViewDef files is transparent to the user and doesn't require any user intervention.

Jinja Syntax and CSO Keywords

The tables below list the Jinja syntax used commonly in configuration templates and the keywords used in configuration templates respectively.

Table 97: Common Jinja Syntax Used in Configuration Templates

Syntax	Explanation
<code>{{ }}</code>	<p>Denotes a variable or expression that will be printed to the template output. For example:</p> <pre>{{tenant_name}}</pre> <p>NOTE: Hyphens are not recognized by the CSO template engine, so use underscores (<code>_</code>) in variables or expressions.</p>
<code>{# #}</code>	<p>Denotes a comment that will not be included in the template output. For example:</p> <pre>{# This is an example of comment in Jinja syntax #}</pre>

Table 97: Common Jinja Syntax Used in Configuration Templates (*continued*)

Syntax	Explanation
{% %}	<p>Denotes statements that are used to create conditional logic:</p> <ul style="list-style-type: none"> The <code>{%- %}</code> statement removes whitespace characters from the output. The <code>if</code> statement used to execute a set of commands (enclosed between the <code>if</code> and <code>endif</code> keywords) when the condition is true. <pre> {% if <condition> %} {% endif %} </pre> The <code>if-else</code> statements are used to execute a set of commands (enclosed between the <code>if</code> and <code>else</code> keywords) when the condition is true and a different set of commands (enclosed between the <code>else</code> and <code>endif</code> keywords) when the condition is false. <pre> {% if <condition> %} {% else %} {% endif %} </pre> The <code>for</code> statement is used to loop through a set of commands (enclosed between the <code>for</code> and <code>endfor</code> keywords) when the condition is true. <pre> {% for <condition> %} {% endfor %} </pre>
Dot (.)	<p>A dot [operator] is used to reference an attribute of a variable. The following example shows a <code>for</code> loop where you can add multiple prefixes:</p> <pre> {% for prefix in Trusted_Network_Prefix_List %} set groups trusted prefix policy options prefix list re ssh {{prefix.Trusted_Network_Prefix_List}} {% endfor %} </pre>

NOTE: You can use configuration template keywords if you enable advanced mode for the configuration template.

Table 98: Configuration Template Keywords

Keyword	Explanation
post_config	Indicates to CSO that the variable that follows is a data type.
pre_config	Indicates to CSO the current configuration associated with a device. The pre_config keyword is used to compare a variable field's value and then modify or delete existing configuration from a target device.
diff_config	Indicates to CSO that the pre_config and post_config should be compared and that CSO should create a new rendered configuration and then push it to target device.

Example 1: Convert a Single Junos OS Command to Jinja Syntax

If you want to convert a single Junos OS command into Jinja syntax for use in a configuration template:

1. Identify the variables that are configured in the Junos OS command.

For example, in the command **set snmp trap-group CSO-Trp-Grp targets 192.0.2.100**, the variables configured are CSO-Trp-Grp and 192.0.2.100.

2. Convert the Junos OS CLI command to Jinja syntax by enclosing each variable in double curly braces as follows: **{{ Variable_Name }}**.

So, in this example, if we use *Trap_Group_Name* and *SNMP_Host_IP_Address* as the variable names, the Jinja syntax for the command is as follows:

```
set snmp trap-group {{ Trap_Group_Name }} targets {{ SNMP_Host_IP_Address }}
```

3. If you paste this in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
SNMP_Host_IP_Addresses
Trap_Group_Name
```

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), using the values indicated in the first step, CSO renders the configuration as follows:

```
delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
edit groups default-domain_Juniper_Test
set snmp trap-group CSO-Trp-Grp targets 192.0.2.100
exit
set apply-groups default-domain_Juniper_Test
```

Notice that although you provided the Jinja syntax for a single Junos OS command, CSO added additional commands to the configuration. This is because, by default, CSO uses Junos OS groups to generate the configuration. Junos OS groups make it easier to apply and delete configurations. For more information, see [Understanding Junos OS Configuration Groups](#).

If you don't want to use Junos OS groups, you must turn on the advanced mode in the configuration template, when you specify the configuration in Jinja syntax..

Example 2: Convert a Junos OS Configuration Snippet to Jinja Syntax

In this example, we'll convert the following Junos OS configuration snippet into Jinja syntax for use in a configuration template:

```
set forwarding-options dhcp-relay server-group DHCP-SERVER 192.0.2.50
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group CSO-Relay-Grp1 interface ge-0/0/2.0
set security zones security-zone trust host-inbound-traffic system-services
dhcp
```

To convert the Junos OS configuration into Jinja syntax:

1. Identify the variables that are configured in the Junos OS commands. For ease of understanding, the variables are enclosed within angular brackets (<>) in the example below.

NOTE: In this example, we're not considering DHCP-SERVER as a variable.

```
set forwarding-options dhcp-relay server-group DHCP-SERVER <Relay_IP>
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group <Relay_Group_Name> interface
<Relay_Interface>
set security zones security-zone <Relay_Zone> host-inbound-traffic
system-services dhcp
```

2. Convert each Junos OS CLI command to Jinja syntax by identifying the variables, providing a name for each variable, and enclosing each variable in double curly braces. So, in this case, the Jinja syntax is as follows:

```
set forwarding-options dhcp-relay server-group DHCP-SERVER {{Relay_IP}}
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group {{Relay_Group_Name}} interface
{{Relay_Interface}}
set security zones security-zone {{Relay_Zone}} host-inbound-traffic
system-services dhcp
```

3. When you paste this in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
Relay_IP
Relay_Interface
Relay_Zone
Relay_Group_Name
```

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), using the values for this example, CSO renders the configuration as follows:

```
delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
```

```

edit groups default-domain_Juniper_Test
set forwarding-options dhcp-relay server-group DHCP-SERVER 192.0.2.50
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group CSO-Relay-Grp1 interface ge-0/0/2.0
set security zones security-zone trust host-inbound-traffic system-services dhcp
exit
set apply-groups default-domain_Juniper_Test

```

Example 3: Use Conditional Logic

In this example, which is a modified version of the preceding example, we'll see how you can use conditional logic (**if** and **for** statements) in a configuration template.

```

{% - if enable_Forwarding_Options %}

set forwarding-options dhcp-relay server-group DHCP-SERVER {{RelayIP }}
set forwarding-options dhcp-relay active-server-group DHCP-SERVER

{% for relay in RelayOptions %}
set forwarding-options dhcp-relay group {{ relay.Relay_Group_Name }} interface {{
relay.Relay_Interface }}
set security zones security-zone {{ relay.Relay_Zone }} host-inbound-traffic
system-services dhcp
{% endfor %}

{% endif %}

```

The explanation of the example above is as follows:

1. In this example, we add an **if** statement and enclose the configuration within that statement as follows:

```

{% - if enable_Forwarding_Options %}

...

...

{% endif %}

```

This means that the configuration is applied only if the `enable_Forwarding_Options` is True. If `enable_Forwarding_Options` is False, then no configuration is applied.

TIP: If you want to apply a different configuration when `enable_Forwarding_Options` is `False`, you can use the **else** statement.

2. Then, we add a **for** statement to enable the configuration of more than one set of values for the **Relay_Group_Name**, **Relay_Interface**, and **Relay_Zone** variables.

```
{% for relay in RelayOptions %}
set forwarding-options dhcp-relay group {{ relay.Relay_Group_Name }} interface
{{ relay.Relay_Interface }}
set security zones security-zone {{ relay.Relay_Zone }} host-inbound-traffic
system-services dhcp
{% endfor %}
```

When you use a **for** statement, the GUI rendered by CSO (when you use the preview feature) displays the variables in table (grid). You can then use the Add icon (+) to add rows to the table and configure one or more sets of values as needed.

3. When you paste the Jinja commands in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
RelayIP
enable_Forwarding_Options

RelayOptions

Relay_Interface
Relay_Zone
Relay_Group_Name
```

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and provide values for the parameters, including two sets of values for **Relay_Group_Name**, **Relay_Interface**, and **Relay_Zone**, CSO renders the configuration as follows:

```
delete groups default-domain_BLR_SOLN_test
delete apply-groups default-domain_BLR_SOLN_test
edit groups default-domain_BLR_SOLN_test
set forwarding-options dhcp-relay server-group DHCP-SERVER 192.0.2.50
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group CSO-RelayGrp1 interface ge-0/0/2.0
```



```

set security zones security-zone trust host-inbound-traffic system-services dhcp
set forwarding-options dhcp-relay group RelayGrp2 interface ge-1/0/2.0
set security zones security-zone untrust host-inbound-traffic system-services
dhcp
exit
set apply-groups default-domain_BLR_SOLN_test

```

Example 4: Use Variable Substitution

In this example, we use a variable as part of the configuration command such that the *value* that we specify for the variable is used in the command.

```

set groups MIST vlans V-{{pool.VLAN_Id}} vlan-id {{pool.VLAN_Id}}

```

The explanation of the example above is as follows:

1. We use the **VLAN_Id** attribute of the **pool** parameter to set the Junos OS configuration parameters **vlans** and **vlan-id**.
2. When you paste the Jinja command **set groups MIST vlans V-{{pool.VLAN_Id}} vlan-id {{pool.VLAN_Id}}** in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```

pool
  VLAN_Id

```

This is because we've used the dot (.) operator to reference the attribute **VLAN_Id** of the parameter **pool**.

3. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and provide the value 120 for **VLAN_Id**, CSO renders the configuration as follows:

```

delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
edit groups default-domain_Juniper_Test
set groups MIST vlans V-120 vlan-id 120
exit
set apply-groups default-domain_Juniper_Test

```

In the rendered configuration command, you can see that the parameters **vlan**s and **vlan-id** are set to **V-120** and **120** respectively, based on the value that we provided for the **VLAN_Id** parameter.

Example 5: Use Filters, Concatenation, and Set Variables

In this example, we'll look at how to set a variable using concatenation and filters, and then use that variable in a Junos OS configuration command.

```
{% set pool_name = Dhcp_Server_Name + '_' + Interface | replace("/", "_") %}
set system services dhcp-local-server overrides process-inform pool {{pool_name}}
```

The explanation of the example above is as follows:

1. The Jinja statement `{% set pool_name = Dhcp_Server_Name + '_' + Interface | replace("/", "_") %}` is used to set a variable called `pool_name`, using two other variables `Dhcp_Server_Name` and `Interface`, as follows:
 - a. The `|` (pipe) operator is used to separate variables from filters, which are functions that modify variables. In this example, we use the `replace("/", "_")` filter to modify the `Interface` variable by replacing the `/` (forward slash) characters with `_` (underscore) characters.
 - b. Then, we use the `+` operator to concatenate the resulting string with the variable `Dhcp_Server_Name`.
2. Then, the Junos OS command `set system services dhcp-local-server overrides process-inform pool {{pool_name}}` is used to configure the Junos OS configuration statement `pool` using the variable `pool_name` that we set in the preceding step.
3. When you paste the Jinja commands in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
Interface
Dhcp_Server_Name
```

As you can see, the Junos OS command or the *pool_name* variables are not displayed because we're using the *Interface* and *Dhcp_Server_Name* variables to arrive at the final Junos OS configuration.

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and provide the values LA_dhcp_srvr for **Dhcp_Server_Name** and ge-0/1/2 for the **Interface**, CSO renders the configuration as follows:

```
delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
edit groups default-domain_Juniper_Test
set system services dhcp-local-server overrides process-inform pool
LA_dhcp_srvr_ge-0_1_2
exit
set apply-groups default-domain_Juniper_Test
```

As explained in a previous step, the / characters in ge-0/1/2 are first replaced with _ characters, which changes the string to ge-0_1_2. This string is concatenated with LA_dhcp_srvr to produce the string LA_dhcp_srvr_ge-0_1_2, which is used in the Junos OS configuration command.

Therefore, the Junos OS configuration command generated is **set system services dhcp-local-server overrides process-inform pool LA_dhcp_srvr_ge-0_1_2**.

Example 6: Test a Value

In this example, we'll look at how to test a value and perform actions based on the result of the test conditions.

```
{%- if NewNetwork.VLAN_Id is defined and (NewNetwork.VLAN_Id | count) > 2 -%}
set vlan-id {{NewNetwork.VLAN_Id}}
{% else %}
set vlans VL-{{NewNetwork.VLAN_Id}}
{% endif %}
```

The explanation of the example above is as follows:

1. We test the parameter **NewNetwork.VLAN_Id** for two conditions:
 - a. Whether the parameter is defined (by using the **NewNetwork.VLAN_Id is defined** condition)
 - b. Whether the length of the parameter is greater than two (by using the condition **(NewNetwork.VLAN_Id | count) > 2**)

Because we use the keyword **and**:

- The configuration command **set vlan-id {{NewNetwork.VLAN_Id}}** is added to the configuration (that CSO generates) when *both* conditions hold true.
 - The configuration **set vlans VL-{{NewNetwork.VLAN_Id}}** is added to the configuration when either of the conditions is false.
2. When you paste the Jinja commands in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
NewNetwork
  VLAN_Id
```

3. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and:

- Provide the value 125 for **VLAN_Id**, CSO renders the configuration as follows because both conditions are true:

```
delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
edit groups default-domain_Juniper_Testset vlan-id 125
exit
set apply-groups default-domain_Juniper_Test
```

- Provide the value 65 for **VLAN_Id**, CSO renders the configuration as follows because one of the conditions is false (length of the parameter is not greater than 2):

```
delete groups default-domain_BLR_SOLN_testtmp
delete apply-groups default-domain_BLR_SOLN_testtmp
edit groups default-domain_BLR_SOLN_testtmp
set vlans VL-65
exit
set apply-groups default-domain_BLR_SOLN_testtmp
```

RELATED DOCUMENTATION

[Add Configuration Templates](#) | 378

View the Configuration Deployed on Devices

In Customer Portal, for any configuration template, users with administrator or operator roles can view the configuration deployed on one more devices.

NOTE: In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

To view the configuration deployed on one or more devices:

1. Select **Resources > Templates > Configuration Templates**.

The Configuration Templates page appears.

2. Navigate to the Devices column of the configuration template for which you want to view the deployed configuration, and click the **Number-of-devices** link.

The Device Configuration page appears.

[Table 99 on page 400](#) explains the fields on this page.

3. After you have viewed the deployed configurations, click **OK**.

You are returned to the Configuration Templates page.

Table 99: Device Configuration Page Fields

Setting	Guideline
Devices	<p>The devices on which the configuration was deployed are displayed in a table. For each device, the following fields are displayed:</p> <ul style="list-style-type: none"> • Device Name • Device Family • Operational Status, indicating whether the device is up or down. • Configuration State: <ul style="list-style-type: none"> • CREATED, indicating that the deployment hasn't started. • DEPLOYED, indicating that the configuration was successfully deployed. • DEPLOYING, indicating that the deployment of the configuration is in progress. • DEPLOY_FAILED, indicating that the deployment of the configuration failed. • Deployment Date, indicating the date and time on which the deployment was triggered. • Job—Click the View logs link for a device to view the deployment history for that device. The Deployment History page appears displaying the number of jobs in progress, number of successful jobs, and number of failed jobs in addition to a table listing some details of the job. You can drill down further by clicking the Regional Log and Log links.
<i>Device-Name</i> Configuration	<p>Select a device by clicking the check box corresponding to the row:</p> <ul style="list-style-type: none"> • For each device on which the configuration deployed successfully, table, this pane displays the configuration that is deployed on the device. • For each device on which the configuration deployment is in progress, DEPLOYING is displayed.

RELATED DOCUMENTATION

[About the Configuration Templates Page](#) | 354

Managing Licenses

IN THIS CHAPTER

- [About the Device Licenses Page | 401](#)
- [Add a Device License File | 403](#)
- [Edit a Device License File | 404](#)
- [Delete a Device License File | 404](#)
- [Push a Device License File | 405](#)
- [About the CSO Licenses Page | 406](#)

About the Device Licenses Page

To access this page, click **Administration > Licenses > Device Licenses**.

You can use the Device Licenses page to view information about the license files and upload the device licenses (.txt format) virtual network services from your local file system. Each license file should contain only one license key. The license key is required to enable application-based routing, application monitoring, and other security features.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a device license file. Click the details icon that appears when you hover over the name of the device license or click **More > Detail**.
- Add device license files. See [“Add a Device License File” on page 403](#).
- Edit device license files. See [“Edit a Device License File” on page 404](#).
- Delete device license files. See [“Delete a Device License File” on page 404](#).
- Push licenses to devices and view history of licenses pushed to a device. See [“Push a Device License File” on page 405](#).

- Filter device license files. Hover over the filter (funnel) icon, click **Add Filter** to specify the filtering criteria, and click **Add**.

The filtered results are displayed on the same page.

- Show or hide columns about the device license. Click the **Show/Hide columns** icon in the top right corner of the page and select the columns that you want to view on the page.
- Search for a device license. Click the **Search** icon in the top right corner of the page to search for a device license.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

Table 100 on page 402 describes the fields on the Device License Files page.

Table 100: Fields on the Device License Files Page

Field	Description
File Name	Name of the device license file. For example, license_Image_v1.
UUID	Displays the universally unique identifier (UUID) of the device license file. For example, xxxxxxxx-xxxx-xxxx-xxx-xxxxxxxxxxxx.
Description	Description of the device license file.
Tenant	Name of the tenant associated with the device license file.
Uploaded	Date and time at which the device license file was uploaded to CSO. For example, 11/18/2016 19:15.
Devices	Displays the number of devices to which the device license file has been pushed. When you hover over the Devices field, you can view the name of the associated devices and their tenants.
Uploaded By	Name of the user who uploaded the license file. For example, test_admin.

RELATED DOCUMENTATION

| [About the Devices Page](#) | 271

Add a Device License File

To add a device license file:

1. Click **Administration > Licenses > Device Licenses**.

The Device License Files page appears.

2. Click the **add** icon (+).

The Add License page appears.

3. In the **License File** field, click **Browse** to navigate to the file location and select the license file.

NOTE: Each license file (.txt format) should contain only one license key.

4. In the **Description** field, enter a description for the license file that you want to upload.

5. Click **OK** to upload the license.

A License Upload job is triggered and you are returned to the Device License Files page.

A confirmation message appears (with the job link) at the top of the page indicating that a job was created. You can click the job link to view the status of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page.

After the job completes successfully, CSO adds the license to the selected devices and the device license file is listed on the Device Licenses File page.

RELATED DOCUMENTATION

| [About the Devices Page](#) | 271

Edit a Device License File

You can only modify the description of a device license file.

To edit the description for the license file:

1. Click **Administration > Licenses > Device Licenses**.

The Device License Files page appears.

2. Select the device license file for which you want to modify the description and click the **Edit** (pencil) icon.

The Edit License page appears.

3. In the **Description** field, update the description for the device license file.

4. Click **OK** to save the changes.

The updated description is visible on the Device License page.

RELATED DOCUMENTATION

[About the Device Licenses Page](#) | 401

Delete a Device License File

To delete a device license:

1. Click **Administration > Licenses > Device Licenses**.

The Device License Files page appears.

2. Select the device license file that you want to delete and click the **delete** (trash can) icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes**.

The device license file is deleted and you are returned to the Device License Files page.

RELATED DOCUMENTATION

| [About the Device Licenses Page](#) | 401

Push a Device License File

You can push licenses to devices from the Device Licenses page of Customer Portal.

To push a license to a device:

1. Click **Administration > Licenses > Device Licenses**.

The Device License Files page appears.

2. Select the device license file that you want to push to a device.

3. Click **Push License > Push**.

The Push License page appears displaying the following information about your sites and devices:

- Site name
- Device name
- Device status
- Status of whether the license is installed on the listed devices or not. If the license is already installed, a green check mark (✓) icon is displayed. If not, a red X is displayed.

NOTE: You can also view the history of licenses pushed on your devices previously by selecting **Push License > Push History**. The Push License History page appears. See [Table 101 on page 406](#).

4. Select the sites and devices to which you want to push the device license file and click **OK**.

An Install License job is triggered and you are returned to the Device License Files page.

A confirmation message appears (with the job link) at the top of the page indicating that a job was created. You can click the job link to view the status of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page.

After the job completes successfully, CSO pushes the license to the selected devices.

Table 101: Fields on the Push License History Page

Field	Description
In Progress	Number of license install jobs that are in progress.
Success	Number of license install jobs that have successfully completed.
Failed	Number of license install jobs that have failed.
Name	Name of the job created to push licenses on the device. You can click on the <i>Name</i> link to view detailed information related to the site history tasks which have successfully completed or failed.
Start Date	Start date and time of license install jobs. The format is MMM/DD/YYYY HH:MM:SS AM/PM.
End Date	End date and time of license install jobs. The format is MMM/DD/YYYY HH:MM:SS AM/PM.
Status	Status of the license install job (success, failed, or in progress).
Log	<p>Link to the logs generated for the license install job. Click on the <i>Log</i> link to view detailed logs about the license install job.</p> <p>The Job Status page appears displaying the date and time at which the license install job and various tasks associated with the job were executed in chronological order.</p>

RELATED DOCUMENTATION

| [About the Device Licenses Page](#) | 401

About the CSO Licenses Page

To access this page, click **Administration > Licenses > CSO Licenses** in Customer Portal.

You can use the CSO Licenses page to view information about the existing CSO licenses assigned to a tenant.

Tasks You Can Perform

You can perform the following tasks from this page:

- Group CSO licenses by sales order or SKUs:

- Click **Group By** and select **Sales Order** to group CSO licenses by sales orders. By default, CSO licenses are grouped by sales order.
- Click **Group By** and select **SKU** to group CSO licenses by SKUs.
- Search for CSO licenses by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
You can search using license SKU, sales order, type, tier, or device class.
- Sort CSO licenses—Click a column name to sort based on the column name.

NOTE: Sorting is applicable only to some fields.

- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the CSO Licenses page.

Field Descriptions

[Table 102 on page 407](#) describes the fields on the CSO Licenses page.

Table 102: Fields on the CSO Licenses page

Field	Description
License SKU	Displays the CSO license SKU name; for example, S-CSO-C-S1-A-3.
Sales Order	Sales order number; for example, 15563238.
Type	Displays whether the license is for an on-premise installation or for a cloud-hosted CSO installation.
Tier	Support tier associated with the license; for example, Standard.
Device Class	Class of the Juniper device associated with the license; for example, B-class.
SSRN	Software support reference number (SSRN), which is necessary to identify your purchase order when you contact Juniper Networks for support
Start Date	Date (in MMM DD , YYYY format) from which the license is valid; for example, Aug 29, 2019.

Table 102: Fields on the CSO Licenses page (continued)

Field	Description
End Date	Date (in MMM DD , YYYY format) up to which the license is valid. CSO calculates the end date based on the validity of the license SKU.
Device Quantity	Total number of on-premise devices that the tenant is authorized to use.
Available	Available number of devices that the tenant can add for the license.
Assigned	This field is not applicable to Customer Portal.

RELATED DOCUMENTATION

| [About the Device Licenses Page](#) | 401

Managing Signature Database and Certificates

IN THIS CHAPTER

- [Signature Database Overview | 409](#)
- [About the Signature Database Page | 410](#)
- [Manually Installing Signatures | 411](#)
- [Automating Signature Database Installation | 413](#)
- [Managing Signature Installation Settings \(Auto Installation\) | 416](#)
- [Certificates Overview | 416](#)
- [About the Certificates Page | 417](#)
- [Importing a Certificate | 419](#)
- [Installing and Uninstalling Certificates | 421](#)
- [About the VPN Authentication Page | 422](#)
- [Modify PKI Settings for All Sites | 425](#)
- [Modify PKI Settings for Selected Sites | 428](#)

Signature Database Overview

The signature database that Juniper provides contains application and intrusion prevention system (IPS) signatures:

- Application signatures are definitions of predefined attacks and applications, and can be used to identify applications for tracking firewall policies and quality-of-service (QoS) prioritization.
- IPS signatures are definitions of predefined attack object and attack object groups that you can use in IDP policies to match traffic against known attacks.

Users with the tenant administrator role can install the active signature database on one or more devices.

RELATED DOCUMENTATION

[About the Signature Database Page | 410](#)

About the Signature Database Page

To access this page, select **Administration > Signature Database**.

Use the Signature Database page to install the active signature database, which contains intrusion prevention system (IPS) and application signatures, on one or more devices. The signature database contains definitions of attacks and application, which are used in defining IPS profile rules and application firewall rules. These attack objects and groups are designed to detect known attack patterns and protocol anomalies within the network traffic.

Tasks You Can Perform

You can perform the following task from this page:

- Install signatures on one or more devices. See [“Manually Installing Signatures” on page 411](#).
- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the Signature Database page.

Field Descriptions

[Table 103 on page 410](#) describes the fields on this page.

Table 103: Fields on the Signature Database Page

Field	Description
Active Database	
Database Version	Version of signature database.
Publish Date	Date and time (YYYY-MM-DD HH:MM:SS 24-hour format) when the signature database was published.
Installed Device Count	Number of devices on which the signature database was successfully installed.
Detectors	Version numbers of the detector engines associated with the signature database. Click the <i>detector-versions</i> link to view the detector details. The Detector Details for <i>Signature-Database-Version</i> page appears displaying (in a table) the platform, OS version, and version of the detectors for the signature database. Click Close to return to the Signature Database page.

Table 103: Fields on the Signature Database Page (*continued*)

Field	Description
Action	<p>Click the Install on device link to install the signatures on one or more devices.</p> <p>The Install Signatures page appears. See “Manually Installing Signatures” on page 411.</p> <p>NOTE: This field appears only for users with the Tenant Administrator role.</p>

RELATED DOCUMENTATION

[Signature Database Overview](#) | 409

Manually Installing Signatures

Users with the tenant administrator role can install the active signature database on one or more devices, by using the on demand signature installation feature. You can install the signature immediately at a click or schedule the installation for a later time. However, you cannot configure a recurring schedule at which installation must be run, unlike the auto installation feature (see [“Automating Signature Database Installation” on page 413](#)). Signatures must be present on the device for application firewall or intrusion prevention system (IPS) features to be used. If you do not install the signature database on a device, the deployment of IPS profiles or application firewall will fail.

NOTE:

- Before you install the signature database on the device, ensure that the IPS license is installed on the device. If the IPS license is not installed, only the application signatures will be installed when the signature database installation is triggered.
- You can install the signature database on the following devices: NFX150, NFX250, SRX Series, and vSRX.

While installing signatures, you can additionally configure settings for installing Intrusion Detection and Prevention (IDP) and enabling micro applications. These settings are applied only to the sites selected.

To install the active signature database:

1. Select **Administration > Signature Database**.

The Signature Database page appears.

2. Click **On Demand Signature Install**.

The **On Demand Signature Installation** page appears displaying the signature database version and the devices on which you can install the signature database.

3. Select the check boxes corresponding to the devices on which you want to install the signature database.

You can also search for, filter, or sort the devices displayed in the table.

4. Enable additional installation options, if required. The following options are available:

- **Install IDP Signature**—Click the toggle button to enable installation of Intrusion Detection and Prevention (IDP) signature database. If the device does not have a valid IDP license installed, the application (App ID) signature is installed. If you have not enabled this option, CSO installs the APP ID signature on the device by default.
- **Enable Micro Apps**—Click the toggle button to configure CSO to identify micro-applications. Enabling this button executes the following set command on the device: **set services application-identification micro-apps**.

5. From the **Type** field:

- Select **Run now** to immediately trigger the installation of the signature database on the devices that you selected.
- Select **Schedule at a later time** to install the signature database later and specify a date and time at which you want the installation to be triggered.

6. Click **OK**.

- If you specified that the database must be installed immediately, a job is triggered and in the Job Tasks page that appears, the tasks associated with the signature database installation are displayed. Click **OK** to exit and return to the Signature Database page.
- If you specified that the database must be installed later, a job is created and you are returned to the Signature Database page. A confirmation message (with the job ID) is displayed at the top of the page.

After the signature database is installed successfully, you can deploy the firewall policy (that references IPS profiles or application signatures) on the device.

RELATED DOCUMENTATION

Automating Signature Database Installation

CSO checks for the availability of new signatures on a daily basis, downloads them when they are available, and then installs these signatures based on the installation settings that you configure by using this page.

As a tenant administrator, you can automate the signature database installation process by configuring the installation settings based on your requirements at the tenant level. You can configure CSO to install the signature database immediately when it is available or specify a recurring schedule at which the installation process must be run. As part of this, you can also configure other options that include settings for alarm generation on completion of the signature installation, micro-application support, and Intrusion Detection and Prevention (IDP) signature installation. You can configure these settings at the all sites, selected sites, or selected site groups levels. However, the configurations at the selected site level overwrite the configurations at the selected site groups and all sites level. The configurations at the selected site groups level overwrite the configurations at the all sites level.

You can also install signatures manually, by using the on demand signature installation feature. For more information, see [“Manually Installing Signatures” on page 411](#).

To configure the signature installation settings:

1. Select **Administration > Signature Database**.

The Signature Database page opens.

2. Click **Auto Installation Settings**.

The **Auto Signature Installation Settings** page opens.

3. Click the add (+) icon.

The **Add Auto Signature Installation Settings** page opens.

4. Complete the configuration settings according to the guidelines provided in [Table 104 on page 414](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

5. Click **OK**.

The settings are saved.

Table 104: Fields on the Add Signature Installation Settings Page

Field	Description
Targets	<p>Select the target type to which you want to apply the signature database installation settings. The following options are available:</p> <ul style="list-style-type: none"> • All Sites • Selected Sites • Selected Site Groups <p>The configurations at the Selected Sites level overwrite the configurations at the All Sites and Selected Site Groups levels. The configurations at the Selected Site Groups level overwrite the configurations at All Sites level.</p> <p>NOTE: You must not duplicate the sites or site groups across multiple installation settings.</p> <p>At a tenant level, you can create only one installation settings with All Sites as target. Similarly, you can create only one installation settings with the same set of site groups or sites.</p>
Site Groups	<p>Available if you have chosen Selected Site Groups as the target type.</p> <p>Select the site groups to which you want to apply the signature installation settings.</p> <p>You can also add the site groups later by editing the settings.</p>
Sites	<p>Available if you have chosen Selected Sites as the target type.</p> <p>Select the sites to which you want to apply the signature installation settings.</p> <p>You can also add the sites later by editing the settings.</p>
Generate Alarms	<p>Click the toggle button to configure CSO to generate an alarm on completion of the signature installation. A successful installation triggers an information alarm. A failed installation triggers a critical alarm.</p>
Enable Micro Apps	<p>Click the toggle button to configure CSO to identify micro-applications. Enabling this button executes the following set command on the device: set services application-identification micro-apps.</p> <p>An example of micro-application is as follows:</p> <p>Consider a dynamic application MODBUS. READ and WRITE are sub functions or operations of MODBUS application. For these sub-functions, we must define micro-applications such as MODBUS-READ and MODBUS-WRITE. In this case, MODBUS is the base application and MODBUS-READ and MODBUS-WRITE are nested applications, that is, micro-applications. By configuring these micro-applications in security policies, you can allow or deny MODBUS sub-functions rather than blocking or allowing the entire MODBUS application.</p>

Table 104: Fields on the Add Signature Installation Settings Page (*continued*)

Field	Description
Install IDP Signature	<p>Click the toggle button to enable installation of Intrusion Detection and Prevention (IDP) signature. If the device does not have a valid IDP license installed, the application (App ID) signature is installed.</p> <p>If you have not enabled this option, CSO installs the APP ID signature on the device by default.</p>
Retry When Device is Up	<p>Click the toggle button to enable CSO to retry installing the signatures on devices where signature installation failed because the host was down (this event triggers a Host Down alarm). CSO retries installation of signatures when the device is up and reachable.</p> <p>You can refer to the install job log to know if the installation (which failed in the first attempt) will be retried.</p>
Install Option	<p>Select an option to specify when to install the new signature when it is available. The following options are available:</p> <ul style="list-style-type: none"> • Install immediately • Install based on a schedule – If you select this option, choose a schedule as well.
Schedule	<p>Select the frequency at which the signatures should be installed.</p> <ul style="list-style-type: none"> • Weekly • Monthly
Days of week	<p>Available only if you have selected the weekly schedule.</p> <p>Select the day(s) on which the signatures should be installed every week.</p>
Days of month	<p>Select the day(s) on which the signatures should be installed every month. If a month has lesser number of days than what is specified, the signature is installed on the last day of the month.</p>
Time	<p>Specify a time at which the installation should be initiated. CSO uses the local time zone.</p>

After the signature database is installed successfully, you can deploy the firewall policy (that references IPS profiles or application signatures) on the device.

RELATED DOCUMENTATION

[Signature Database Overview | 409](#)

[About the Signature Database Page | 410](#)

Managing Signature Installation Settings (Auto Installation)

You can edit or delete the signature installation settings

To edit or delete the signature installation settings:

1. Select **Administration > Signature Database**.

The Signature Database page opens.

2. Click **Auto Installation Settings**.

The **Auto Signature Installation Settings** page opens.

3. Select the installation setting that you want to edit, and then click:

- The edit button (the pencil icon) to edit the signature installation setting. See [“Automating Signature Database Installation” on page 413](#) for more information about the fields on the screen.
- The delete button to delete the signature installation setting.

RELATED DOCUMENTATION

[Managing Signature Installation Settings \(Auto Installation\) | 416](#)

[Signature Database Overview | 409](#)

[About the Signature Database Page | 410](#)

Certificates Overview

SSL uses public-private key technology that requires a private key paired with an authentication certificate for the SSL service. An SSL certificate includes identifying information such as a public key and a signature issued by a certificate authority (CA).

CAs are entities that validate identities and issue certificates. A CA can issue multiple certificates in the form of a tree structure. A root certificate is the topmost certificate of the tree, the private key of which is used to sign other certificates. All certificates immediately below the root certificate inherit the signature or trustworthiness of the root certificate. This is somewhat like the notarizing of an identity. You can configure a root CA certificate by first obtaining a root CA certificate (by either generating a self-signed one or importing one) and then applying it to an SSL proxy profile.

NOTE: SSL certificates are used for the SSL forward proxy feature in CSO.

RELATED DOCUMENTATION

[SSL Forward Proxy Overview | 710](#)

[About the SSL Proxy Profiles Page | 727](#)

About the Certificates Page

To access this page, select **Administration > Certificates** in Customer Portal.

Use this page to view and manage SSL certificates. You can import a root certificate or a trusted certificate (directly from a file or by pasting the content) and install a certificate on a site.

Tasks You Can Perform

You can perform the following tasks from this page:

- View information about the existing certificates; see [Table 105 on page 418](#).
- Import a certificate—Select **More > Import Certificate**. See [“Importing a Certificate” on page 419](#).
- View the sites on which a certificate is installed—Select a certificate and then select **More > View Installed Sites**.

The View Installed Sites page appears, displaying the list of sites on which the selected certificate is installed. Click **OK** to close the page and return to the Certificates page.

- Install a certificate on a site—Select a certificate and then select **More > Install Certificate**. See [“Installing and Uninstalling Certificates” on page 421](#).
- Uninstall a certificate from a site—Select a certificate and then select **More > Uninstall Certificate**. See [“Installing and Uninstalling Certificates” on page 421](#).
- View details about a certificate—Select a certificate and then select **More > Detailed View**. The Detailed View page appears. See [Table 106 on page 418](#) for an explanation of fields on this page.

Field Descriptions

[Table 105 on page 418](#) displays the fields on the Certificates page.

Table 105: Fields on the Certificates Page

Field	Description
Certificate Name	Name of the certificate.
Type	Type of the certificate: <ul style="list-style-type: none"> • Root certificate • Trusted certificate
Description	Description of the certificate.

Table 106: Fields on the Detailed View Page

Field	Description
Certificate Name	See Table 105 on page 418 .
Type	See Table 105 on page 418 .
Valid From	Date and time (UTC) from which the certificate is valid.
Valid Upto	Date and time (UTC) until which the certificate is valid.
Serial Number	Serial number of the certificate.
Signature Algorithm	Algorithm used to sign the certificate.
Issuer Details	Details of the authority that issued the certificate, including details such as name, country, organization, and so on.
Version	X.509 version of the certificate.

RELATED DOCUMENTATION

[About the SSL Proxy Profiles Page](#) | 727

Importing a Certificate

You can import an SSL certificate (directly from a file or by pasting the content) from the Import Certificate page.

NOTE: If you want to use the SSL proxy feature, you must import at least one root certificate for a tenant; the certificate can be used in one or more sites.

To import a certificate:

1. Select **Administration > Certificates** in Customer Portal.

The Certificates page appears.

2. Select **More > Import Certificate**.

The Import Certificate page appears.

3. Complete the configuration according to the guidelines provided in [Table 107 on page 419](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to import the certificate.

You are taken to the Certificates page. If the certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

After importing a certificate, you can use it when you create an SSL proxy profile.

Table 107: Import Certificate Settings

Setting	Guideline
Certificate Name	Enter the certificate name, which must be a unique string of alphanumeric characters and some special characters (_ -). No spaces are allowed and the maximum length is 32 characters.
Certificate Type	Select an option to specify whether the certificate that you are importing is a root certificate (Root CA) or a trusted certificate (Trusted CA).


```
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
-----END CERTIFICATE-----
```

RELATED DOCUMENTATION

[Installing and Uninstalling Certificates | 421](#)

[Creating SSL Forward Proxy Profiles | 729](#)

Installing and Uninstalling Certificates

IN THIS SECTION

- [Installing a Certificate | 421](#)
- [Uninstalling a Certificate | 422](#)

You can install and uninstall certificates from the Certificates page. This topic has the following sections:

Installing a Certificate

Use the Install Certificate page to install certificates on one or more sites.

To install a certificate on one or more sites:

1. Select **Administration > Certificates** in Customer Portal.

The Certificates page appears, displaying the existing certificates.

2. Select the certificate that you want to install, and then select **More > Install Certificate**. Alternatively, right-click a certificate and select **Install Certificate**.

The Install Certificate page appears, displaying a list of sites.

3. Select the sites on which you want to install the certificate.
4. Click **Install** to install the certificate on the selected sites.

You are taken to the Certificates page. A job is created and a confirmation message appears with the ID of the job. Click the job ID to go to the Jobs page, where you can view the status of the job.

Uninstalling a Certificate

If a certificate's validity has expired or if you want to remove a certificate from a site, you can uninstall the certificate from that site.

To uninstall a certificate from one or more sites:

1. Select **Administration > Certificates** in Customer Portal.

The Certificates page appears, displaying the existing certificates.

2. Select the certificate that you want to uninstall, and then select **More > Uninstall Certificate**.
Alternatively, right-click a certificate and select **Uninstall Certificate**.

The Uninstall Certificate page appears, displaying only those sites on which the certificate was previously installed.

3. Select the sites from which you want to uninstall the certificate.

4. Click **Uninstall** to uninstall the certificate from the site.

You are taken to the Certificates page. A job is created and a confirmation message appears with the ID of the job. Click the job ID to go to the Jobs page, where you can view the status of the job.

RELATED DOCUMENTATION

| [Importing a Certificate](#) | 419

About the VPN Authentication Page

IN THIS SECTION

- [Tasks You Can Perform](#) | 423
- [Field Descriptions](#) | 423

Contrail Service Orchestration (CSO) establishes secure IPsec Virtual Private Network (VPN) tunnels to connect sites after authenticating the tunnel endpoints. CSO authenticates tunnel endpoints by using either preshared keys or Public Key Infrastructure (PKI) certificates.

Service Provider (SP) and Operating Company (OpCo) Administrators can configure the authentication type when the tenant is onboarded.

If PKI certificate is configured as the authentication type, then tenant administrators can modify the PKI settings from the VPN Authentication page (**Administration > Certificate Management > VPN Authentication**) after the tenant is onboarded.

NOTE: The VPN Authentication page is displayed only for tenants with SD-WAN service that are configured with PKI as the authentication type.

Tasks You Can Perform

- View information about the existing certificates for all provisioned sites in the tenant. See [Table 108 on page 424](#).
- Change the Certificate Authority (CA) server settings (URL, password, and CRL Server URL) for the tenant. See [“Modify PKI Settings for All Sites” on page 425](#).
- Change the Certificate Revocation List (CRL) URL of certificates for the tenant. See [“Modify PKI Settings for All Sites” on page 425](#).
- Change the method of renewing PKI certificates for all provisioned sites in the tenant. See [“Modify PKI Settings for All Sites” on page 425](#).
- Change the method of renewing PKI certificates for one or more provisioned sites in the tenant. See [“Modify PKI Settings for Selected Sites” on page 428](#).
- Manually renew certificates for one or more provisioned sites in the tenant. See [“Modify PKI Settings for Selected Sites” on page 428](#).
- Search for certificates by using keywords. Click the **Search** icon to enter the search term in the text box and press **Enter**. The search results are displayed on the same page.
- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the grid and select the columns that you want displayed on the VPN Authentication page.

Field Descriptions

[Table 108 on page 424](#) describes the fields on the VPN Authentication page.

Table 108: Fields on the VPN Authentication page

Field	Description
<i>Tenant-Level Settings for PKI Certificates</i>	
Certificate Renewal	
Current Tenant Setting	Renewal method currently configured for PKI certificates of the tenant.
Next Renew Check Time	<ul style="list-style-type: none"> • If the Auto Renew Certificate toggle button on the Edit Tenant Certificate page is enabled, displays the date and time at which the next renewal check is scheduled. • If the Auto Renew Certificate toggle button on the Edit Tenant Certificate page is disabled, displays N/A (not applicable).
Next CRL check time	Date and time at which the next CRL check is scheduled.
Last CRL update time	Date and time at which the CRL was last updated.
<i>Details of Certificates</i>	
Tenant Name	Name of the tenant.
Common Name	Name of the PKI certificate.
Certificate ID	ID of the PKI certificate.
Serial Number	Serial number of the PKI certificate.
Used In	Name of the site with which the PKI certificate is associated.
Device	Name of the device with which the PKI certificate is associated.

Table 108: Fields on the VPN Authentication page (*continued*)

Field	Description
Status	<p>Expiration status of the PKI certificate:</p> <ul style="list-style-type: none"> • If you set the certificate to be renewed automatically, the status displayed depends on the renewal period that you selected from the Edit Certificate Settings for Tenant page. For example, if you selected the renewal period as 1 month, the Status field displays Less than 1 month before expiry. • If you set the certificate to be manually renewed, the status displayed depends on the expiration notification time for the certificate (Status: Less than 2 weeks before expiry). • If the expiration date of the certificate does not meet the expiration notification time yet, the Status field displays –. • If the certificate has expired, the Status field displays Expired.
Expires on	Date and time at which the PKI certificate expires.
Renewal Method	<p>Renewal method of the PKI certificate:</p> <ul style="list-style-type: none"> • Auto • Manual

RELATED DOCUMENTATION

[View and Edit Tenant Settings](#) | 27

Modify PKI Settings for All Sites

The VPN authentication settings for a tenant are configured when the tenant is onboarded. If PKI Certificate is configured as the authentication type, tenant administrators can modify the PKI settings even after adding sites for the tenant. The changed settings are applicable to all existing sites of the tenant and to sites that the tenant might add later.

You can modify the following PKI settings from the Edit Certificate Settings for Tenant page (**Administration > Certificate Management > VPN Authentication > Change**).

- **Certificate Authority (CA) Server Parameters**

The CA server manages the lifecycle of a certificate and publishes revoked certificates to the Certificate Revocation List (CRL) server. To obtain trusted CA certificates, CSO communicates with the CA server using the Simple Certificate Enrollment Protocol (SCEP).

To change the CA server parameters (URL, Password, and CRL URL):

1. On the Edit Certificate Settings for Tenant page, enter the new CA server URL and password in the **CA Server URL** and **Password** fields, respectively. Enter the new CRL server URL associated with the CA server in the **CRL Server** field.
2. Click **OK** to save your changes.

You are returned to the VPN Authentication page, where a confirmation message appears indicating that a job is triggered to automatically renew certificates for all sites in the tenant.

You can click the job link in the message to view the job details, or view the details on the Jobs (**Monitor > Jobs**) page.

NOTE: The CA server parameters are not updated if the PKI server is unreachable at the time that the job is triggered.

After the job is completed successfully, a confirmation message appears indicating that the settings are updated. CSO also downloads the latest list of revoked certificates from the CA server.

• CRL Server URL

You can choose to update only the CRL server URL associated with the CA server.

To update the CRL server URL:

1. On the Edit Certificate Settings for Tenant page, specify the new CRL server URL in the **CRL Server** field.
2. Click **OK** to save your changes.

You are returned to the VPN Authentication page, where a confirmation message appears indicating that a job is triggered.

You can click the job link in the message to view the job details or view the details on the Jobs (**Monitor > Jobs**) page.

After the job is completed successfully, a confirmation message appears indicating that the settings are updated. CSO downloads the latest list of revoked certificates from the CA server.

• Certificate Renewal Method

To change the certificate renewal method:

1. On the Edit Certificate Settings for Tenant page, click the Auto Renew Certificate toggle button to enable or disable the automatic renewal of certificates.
2. If you enable the Auto Renew Certificate toggle button, the **Renew Before Expiry** list appears.

From the list, select the period before the expiry date on which the certificates should be automatically renewed:

- 3 Days
- 1 Week
- 2 Weeks (default)
- 1 Month

If you disable the Auto Renew Certificate toggle button, the certificates should be manually renewed for each site before they expire. See [“Modify PKI Settings for Selected Sites” on page 428](#) for the procedure to manually renew certificates for sites.

3. Click **OK** to save your changes.

If you enabled the automatic renewal of certificates, CSO schedules a job to check the expiration date of certificates for all sites of the tenant (every 24 hours). Based on the expiration date that you’ve configured, CSO triggers a job to automatically renew the certificates.

NOTE: The certificate renewal job is not executed for sites that are down or that do not have connectivity to CSO at the time that the job is triggered.

You are returned to the VPN Authentication page where a confirmation message appears indicating that the settings are updated.

RELATED DOCUMENTATION

[About the VPN Authentication Page | 422](#)

[View and Edit Tenant Settings | 27](#)

Modify PKI Settings for Selected Sites

The VPN authentication settings for a tenant are configured when the tenant is onboarded. If PKI Certificate is configured as the authentication type, tenant administrators can modify the PKI settings even after adding sites for the tenant. The changed settings are applicable to all existing sites of the tenant and to sites that the tenant might add later. To change the PKI settings for all sites in the tenant, see [“Modify PKI Settings for All Sites” on page 425](#).

You can perform the following actions on the selected sites:

- Change the method of renewing PKI certificates:

NOTE: You can change the renewal method of PKI certificates for sites in a tenant only if you set the certificate renewal method for the tenant to automatic (that is, if you enable the Auto Renew Certificate toggle button).

Do the following:

1. Select **Administration > Certificate Management > VPN Authentication**.

The VPN Authentication page appears.

2. Select one or more sites from the list of available sites and click **Change Renewal Method**.

A drop-down list appears.

3. From the list, choose the renewal method (**Set Auto Renew** or **Set Manual Renew**).

The **Edit Certificate Renewal Method** page appears asking you to confirm the renewal method.

4. Click **Yes** to change the renewal method.

You are returned to the VPN Authentication page, where a confirmation message appears indicating that the certificate renewal method is updated. The Renewal method column on the VPN Authentication page displays the updated renewal method for the selected sites.

- Manually renew certificates:

1. Select **Administration > Certificate Management > VPN Authentication**.

The VPN Authentication page appears.

2. Select one or more sites from the list of available sites and click **Renew Certificate**.

The Confirm Renew Certificate page appears.

3. Click **Yes** to manually renew the certificates.

You are returned to the VPN Authentication page, where a confirmation message appears indicating that a certificate renewal job is triggered.

You can click the job link in the message to view the job details, or view the details on the Jobs (**Monitor > Jobs**) page.

NOTE: The certificate renewal job is not executed for sites that are down or that do not have connectivity to CSO at the time that the job is triggered.

If the job is completed successfully, a confirmation message appears on the VPN Authentication page.

RELATED DOCUMENTATION

[About the VPN Authentication Page | 422](#)

[View and Edit Tenant Settings | 27](#)

Managing Juniper Identity Management Service

IN THIS CHAPTER

- [Juniper Identity Management Service Overview | 430](#)
- [About the Identity Management Page | 433](#)
- [Configuring CSO and JIMS Connection | 434](#)
- [Configuring JIMS for an SRX Device | 436](#)

Juniper Identity Management Service Overview

IN THIS SECTION

- [Access Token Query | 431](#)
- [Batch or Periodic Query | 431](#)
- [IP Address Query | 432](#)
- [User Mapping Query | 432](#)

Juniper Identity Management Service (JIMS) provides a robust and scalable user identification and IP address mapping implementation that includes endpoint context and machine ID. JIMS collects user identity information from different authentication sources, for SRX Series devices.

JIMS collects user identity information from a configured Active Directory and makes it available to SRX Series devices or vSRX instances. You can download and install Juniper Identity Management Service (JIMS), configure the CSO client on JIMS to obtain user identity information from the configured Active Directory, and use CSO and JIMS to manage user-based firewall policy intents on SRX Series devices and vSRX instances.

The SRX Series devices communicate with JIMS through HTTP or HTTPS connection. Use HTTP connection for debugging and HTTPS for deployments. SRX Series devices consist of primary and secondary JIMS configurations. These devices must always query the primary JIMS. The secondary JIMS is available as a

fall back option with limited resources. The secondary JIMS must be used when the HTTP GET query or a number of queries to the primary JIMS fails. SRX Series devices constantly scrutinize the failed primary JIMS and revert to the primary JIMS, once it is up and running.

When you request a JIMS report, the SRX Series device specifies the timestamp. JIMS forms an HTTPS response from the earliest known report since the requested timestamp. SRX Series devices request for the maximum number of reports to include in the response from JIMS. Along with the requested reports, JIMS always returns a cookie. In the subsequent requests to JIMS, SRX Series devices include cookies instead of timestamp to indicate the same context, same beginning timestamp, and to resume the same response from where it has stopped the previous time.

NOTE:

- IP and user mapping information might be inaccurate, if the user identities in JIMS are cleared, delayed, or missing.
- SRX firewall authentication can also push the authentication entries to JIMS.

The SRX Series device communicates with JIMS through HTTP or HTTPS messages to obtain the access token and query for user identities. The following different query modes are available and all queries can happen simultaneously.

Access Token Query

JIMS requires OAuth 2.0 protocol to authenticate or authorize. The SRX Series device user query function requires an access token to query the JIMS server. The SRX Series device uses the client credentials such as client ID and client secret to obtain an access token. These parameters must be consistent with the API client configured on JIMS.

Batch or Periodic Query

At the beginning, SRX Series device sends the batch queries to JIMS sequentially to obtain all the expected user identities. When there are no more entries in JIMS, SRX Series device periodically queries for the newly generated reports with the configured interval.

The timestamp is mentioned in the query to restart the response. The timestamp is expected in the query under the following circumstances:

- SRX Series device queries the JIMS server for the first time
- SRX Series device switches over to the secondary JIMS
- SRX Series device does the error recovery because of an internal error or upon receiving error response from JIMS

For all the other cases, SRX Series device provides the received cookie information in the query instead of a timestamp.

IP Address Query

SRX Series device can provide another query to JIMS specifying the IP address, if it has missed the data for the existing IP address flow. If there are many IP address queries in the queue, SRX Series device can keep multiple concurrent HTTP or HTTPS connections with JIMS to increase the throughput. However, the number of concurrent connections are restricted to less than or equal to 20 connections to reduce the load on JIMS.

User Mapping Query

SRX Series device can engage Captive Portal to obtain the user ID to authenticate the user. Once the user is authenticated, SRX Series device can issue another query to JIMS specifying the user ID and IP address to obtain user information. The firewall authentication uses the `https://<JIMS>/<query-api>/user/ip=<ip>&id=<id>&domain=<domain>` API to push an authentication success entry to JIMS with the user IP, user ID, and the domain. JIMS responds with the user information.

The difference between the IP address query and user query is that the IP address query does not have the user ID. Both these queries insert the user information to the internal cache of JIMS , and all SRX devices are updated with user information.

RELATED DOCUMENTATION

[About the Identity Management Page | 433](#)

[Configuring CSO and JIMS Connection | 434](#)

[Configuring JIMS for an SRX Device | 436](#)

About the Identity Management Page

To access this page, select **Administration > Identity Management**.

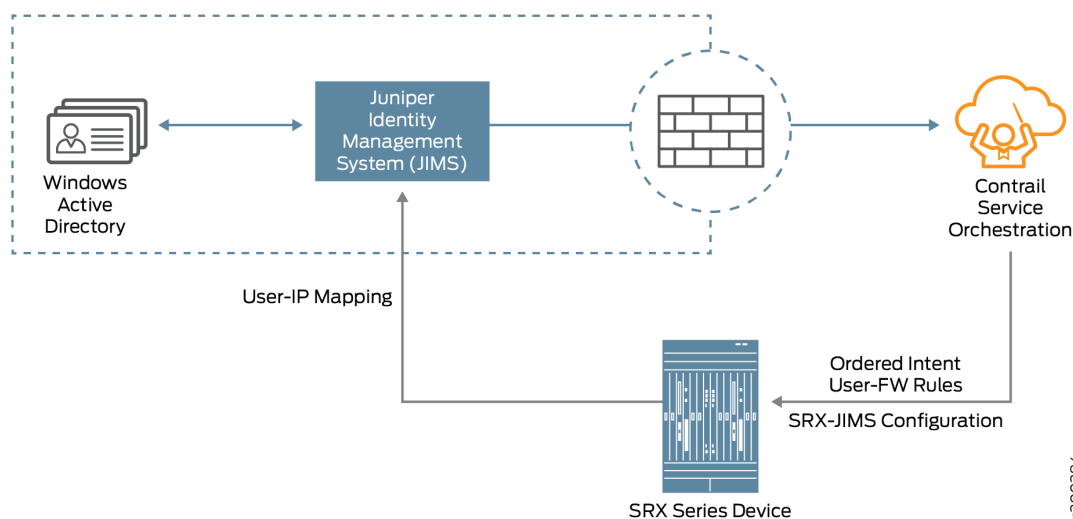
NOTE:

- For information on system requirements for installing JIMS, see [System Requirements for Installing Juniper Identity Management Service](#)
- For information on installing JIMS on your Windows server, see [Installing Juniper Identity Management Service](#).

Use the **Identity Management** page to download and install JIMS, interface JIMS with CSO to obtain advanced user identity an active directory, and use CSO to push the JIMS configuration to SRX Series devices.

[Figure 18 on page 433](#) illustrates the connectivity between, CSO, JIMS, and an SRX Series device.

Figure 18: CSO-JIMS-SRX Connectivity Configuration



Tasks You Can Perform

You can perform the following tasks from this page:

- Download the JIMS executable to your Windows server using **Download JIMS**. Run the JIMS executable to install JIMS on your Windows server machine. See [System Requirements for Installing Juniper Identity Management Service](#) and [Installing Juniper Identity Management Service](#).

After you have successfully installed JIMS, you can login into JIMS using your Windows user ID and password.

- Configure the connection between CSO and JIMS to import user and group lists from an Active Directory (AD) of your choice, using **JIMS to CSO**. See [“Configuring CSO and JIMS Connection” on page 434](#).
- Configure the connection between JIMS and an SRX Series device. See [“Configuring JIMS for an SRX Device” on page 436](#).

RELATED DOCUMENTATION

[Juniper Identity Management Service Overview | 430](#)

[Configuring CSO and JIMS Connection | 434](#)

[Configuring JIMS for an SRX Device | 436](#)

[Preparing CSO Identity Management](#)

[JIMS v1.1 Feature Guide](#)

Configuring CSO and JIMS Connection

Before you begin to configure the connection between CSO and JIMS, ensure that you have downloaded and installed JIMS. See [System Requirements for Installing Juniper Identity Management Service](#) and [Installing Juniper Identity Management Service](#).

To configure a connection between CSO and JIMS:

1. Select **Administration > Identity Management**.

The **Identity Management** page appears.

2. Click **JIMS-to-CSO Configuration** or the greater-than (>) symbol beside it.

The **JIMS-to-CSO Configuration** panel expands. The panel displays a system-generated user name which cannot be changed, the last updated time of the user identity information from Active Directory and the connection status of the JIMS server(s).

NOTE: If you have already configured a JIMS user account in CSO, the details of this connection is displayed in the **JIMS-to-CSO Configuration** panel.

3. The **Username** is auto-generated for each tenant. You will not be able to change it. Enter a password of your choice for your JIMS-to-CSO connection in the **Password** field.

NOTE: The password must contain a number, an upper-case letter, and a special character.

NOTE: The password you entered will appear encrypted. If you want to see the password that you entered as plain text, select **Show Password**.

4. Click **Save** to save your changes. The JIMS user credentials are saved.
If you do not want to save your changes, click **Cancel**.
5. CSO and JIMS need to be connected in order for JIMS to push data to CSO. To set up this connection, you must configure the CSO client on JIMS, using the username and password that you created in the **JIMS-to-CSO Configuration** panel. For more information on configuring the CSO client on JIMS, see [Configuring the Connection to a CSO Client](#).
6. Configure an Active Directory (AD) as a data source in JIMS, see [Configuring the Connection to an Active Directory](#).

NOTE: After your JIMS user credentials are saved, the password field changes to the **Change Password** link.

If you want to change your password, click **Change Password**.

The **Change Password** page appears.

- Enter your new password in the **New Password** field and re-enter the same password in the **Confirm Password** field.
- Click **OK** to save the new password. The updated password is saved.

If you do not want to save your new password, click **Cancel** instead.

RELATED DOCUMENTATION

Configuring JIMS for an SRX Device

Configuring the connection between SRX Series devices to JIMS allows the JIMS server to send the IP address, username, and group relationship information to SRX Series devices through CSO. You can also configure a set of optional advanced settings for authentication timeout, domain filters, and choose to include or exclude user identity information in the communication between the JIMS server and the SRX Series device.

For every SRX Series device, you can configure the primary and secondary JIMS servers. The SRX Series device always queries the primary JIMS server. The secondary JIMS server is available as a fallback option with limited resources. The secondary JIMS server is used when a number of queries to the primary JIMS server fails. The SRX Series device constantly scrutinizes the failed primary JIMS server and reverts to the primary JIMS server, once it is up and running.

Before you begin, you need the following information:

- The IP address of the primary and secondary (optional) JIMS server.
- The client ID to obtain an OAuth token from the JIMS server for user queries.
- The client secret to obtain an OAuth token from the JIMS server for user queries.

To configure a connection between an SRX Series device and JIMS:

1. Select **Administration > Identity Management**.

The **Identity Management** page appears.

2. Click **SRX-to-JIMS Configuration** or the greater-than (>) symbol beside it.

The **SRX-to-JIMS Configuration** panel expands.

NOTE: If you have already configured JIMS for an SRX Series device, the details of this configuration is displayed in the **SRX-to-JIMS Configuration** panel.

3. Complete the configuration according to the guidelines provided in [Table 109 on page 437](#).
4. Click **Save** to save the changes. JIMS is now configured for an SRX device.

If you want to discard your changes, click **Cancel** instead.

Table 109 on page 437 provides guidelines on using the fields on the **SRX-to-JIMS Configuration** panel.

Table 109: Fields on the SRX-to-JIMS Configuration Panel

Field	Description
Identity	
IP Address	<p>Enter a valid IPv4 or IPv6 address of the primary JIMS server.</p> <p>SRX Series devices always query the primary JIMS to obtain the user identities.</p>
Secondary Identity	<p>Enable this option to use the secondary JIMS server as a fallback when the primary JIMS server fails. By default, this option is disabled.</p>
Secondary IP Address	<p>Enter a valid IPv4 or IPv6 address of the secondary JIMS server.</p> <p>The secondary JIMS is available as a fall back option with limited resources. Use the secondary JIMS when the HTTP GET query or number of queries to the primary JIMS fails.</p>
Client Credentials	
Client ID	<p>Enter the client ID that the SRX Series device provides to JIMS server as part of its authentication. The SRX Series device must authenticate itself with the JIMS server to obtain an access token that allows the it to query the JIMS server for user identity information. The client ID must be consistent with the CSO client ID or username configured on the JIMS server.</p>
Client Secret	<p>Enter the client secret that the SRX Series device provides to the JIMS server as part of its authentication. The client secret must be consistent with the CSO client secret or password configured on the JIMS server.</p>
Advanced Settings	
Authentication Entry Timeout	<p>Enter the timeout interval (in minutes) after which, the idle entries in the JIMS authentication table expire. The timeout interval begins from when the user authentication entry is added to the authentication table. This value can be between 10 and 1440 minutes, where a value of 0 means no timeout. The default value is 69 minutes.</p>
Include IP Address(es)	<p>The SRX Series device sends a query to JIMS for the user identity information only for the IP addresses present in the selected address group; JIMS responds with the requested user identity information.</p> <p>Click Add New Address to create a new IP address group, see “Creating Addresses or Address Groups” on page 753.</p>

Table 109: Fields on the SRX-to-JIMS Configuration Panel (*continued*)

Field	Description
Exclude IP Address(es)	<p>The SRX Series device does not query JIMS for the user identity information for the excluded IP addresses present in the selected address group.</p> <p>Click Add New Address to create a new IP address group, see “Creating Addresses or Address Groups” on page 753.</p>
Filter Domain(s)	<p>The SRX Series device sends a query to JIMS for the user identity information within the specified domains. Enter a comma-separated list of up to 25 domain names. A domain name can be an alphanumeric string of up to 64 characters that can also contain dashes, underscores, and dots.</p> <p>Example: example.net</p>

RELATED DOCUMENTATION

[Juniper Identity Management Service Overview | 430](#)

[About the Identity Management Page | 433](#)

[Configuring CSO and JIMS Connection | 434](#)

4

PART

Managing Policies, Profiles, and Proxies

Managing Firewall Policies | **440**

Managing UTM Profiles | **518**

Managing SLA Profiles and SD-WAN Policies | **567**

Managing NAT Policies | **628**

Managing IPS Signatures and Profiles | **665**

Managing SSL Proxies | **710**

Deploying Policies | **738**

Managing Firewall Policies

IN THIS CHAPTER

- Firewall Policy Overview | 441
- About the Firewall Policy List Page | 443
- About the Firewall Policy Name Page | 444
- Adding a Firewall Policy | 445
- Editing and Deleting Firewall Policies | 447
- Adding Firewall Policy Intents | 449
- Editing, Cloning, and Deleting Firewall Policy Intents | 455
- Selecting Firewall Source | 457
- Selecting Firewall Destination | 461
- Firewall Policy Examples | 464
- Firewall Policy Schedules Overview | 504
- About the Firewall Policy Schedules Page | 505
- Creating Schedules | 506
- Editing, Cloning, and Deleting Schedules | 508
- Deploying Firewall Policies | 509
- About the Default Profiles for Unified Firewall Policy Page | 510
- Editing Default Settings for the Unified Firewall Policy | 512
- Importing Policies Overview | 514
- Importing Firewall Policies | 516

Firewall Policy Overview

Contrail Service Orchestration (CSO) provides the ability to create, modify, and delete firewall policy intents associated with a firewall policy. Firewall policies are presented as *intent-based policies*. A firewall policy intent controls transit traffic within a context that is derived out of the end-points defined in the intent. Intent-based firewall policies can incorporate both transport layer (Layer 4) and application layer (Layer 7) firewall constructs in a single intent. The underlying system, automatically analyzes the intent, translates them into the set of rules the devices understand. The choice of sequence and the assignment happens implicitly based on the endpoints in the intent definition. The intent consist of source and destination endpoints. Endpoints could be applications (L7), sites or site groups, IP address/address-groups, services, or departments.

NOTE:

- Starting from CSO Release 5.0.1, if a device (CPE or next-generation firewall) is running Junos OS Release 18.2R1 or later, a firewall policy acts as a unified firewall policy. In a unified firewall policy, dynamic application can be used as a match condition along with the existing match conditions. Therefore, a separate application firewall is not configured on the device to allow or block traffic to an application.

However, If the device is running a version earlier than Junos OS Release 18.2R1, the firewall policy does not act as a unified firewall policy and application firewalls continue to be configured on the device.

See [Unified Security Policies](#) for information about unified firewall policies.

Firewall policies provide security functionality by enforcing intents on traffic that passes through a device. Traffic is permitted or denied based on the action defined as the firewall policy intent.

A firewall policy provides the following features:

- Permits, rejects, or denies traffic based on the application in use.
- Identifies not only HTTP but also any application running on top of it, enabling you to properly enforce policies. For example, an application firewall intent could block HTTP traffic from Facebook but allow Web access to HTTP traffic from Microsoft Outlook.
- Provides the ability to enable advanced security protection by specifying one or more of the following:
 - Unified threat management (UTM) profile
 - SSL proxy profile
 - Intrusion prevention system (IPS) profile

In CSO, intents are categorized as zone-based intents and enterprise-based intents.

- Zone-based-intents are intents with zones as source and destination endpoints. The policies with zone-based intents can be applied to SD-WAN sites and next-generation firewall sites. The parameters that you can define for zone-based intents are listed in [Table 110 on page 442](#).

Table 110: Zone-based intents

Source End Points	Destination End points	Advanced Security Options	Supported Options
Zones	Zones	SSL Proxy Profile	Scheduler
Address	Address	UTM Profile	Logging
Users	Service (L4 port/protocol) Applications (Dynamic Applications)	IPS Profile	

NOTE: You cannot select a department or site as an endpoint in zone-based intents. The sites assigned to the policy are applicable for zone-based intents and are automatically considered for deployment.

- Enterprise-based intents are intents that contain sites, site-groups, departments, addresses as source and destination endpoints. Firewall policies with enterprise-based intents can be applied only to SD-WAN sites. The parameters that you can define for enterprise-based intents are listed in [Table 111 on page 442](#).

Table 111: Enterprise-based intents

Source Endpoints	Destination Endpoints	Advanced Security Options	Supported Options
Sites	Sites	UTM Profile	Scheduler
Site-groups	Site-groups	IPS Profile	Logging
Departments	Departments		
Addresses	Addresses		
Users	Users Service/Applications		

NOTE:

- Zones cannot be selected as source or destination endpoints for enterprise-based intents.
- Intents added in CSO Release 4.1 and earlier are now called enterprise-based-intents.

RELATED DOCUMENTATION

About the Firewall Policy Name Page 444
Firewall Policy Examples 464
Adding Firewall Policy Intents 449
Editing, Cloning, and Deleting Firewall Policy Intents 455

About the Firewall Policy List Page

To access this page, select **Configuration > Firewall > Firewall Policy**.

Use this page to view and manage firewall policies associated with your site or site groups.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a firewall policy. See [“Adding a Firewall Policy” on page 445](#).
- Edit or delete a firewall policy. See [“Editing and Deleting Firewall Policies” on page 447](#).
- Import a firewall policy. See [“Importing Firewall Policies” on page 516](#).
- Deploy a firewall policy. See [“Deploying Firewall Policies” on page 509](#).
- Search for a firewall policy. Click the Search icon in the top right corner of the page to search for a firewall policy.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

[Table 112 on page 443](#) provides guidelines on using the fields on the **Policy List** page.

Table 112: Fields on the Policy List Page

Field	Description
Policy Name	Name of the firewall policy.
Number of intents	Number of intents associated with the firewall policy.
Applied to	Sites to which the firewall policies are applied.

Table 112: Fields on the Policy List Page (continued)

Field	Description
Status	Status of firewall policy deployment.

RELATED DOCUMENTATION

| [Firewall Policy Overview](#) | 441

About the Firewall Policy Name Page

To access this page, select **Configuration > Firewall > Firewall Policy** and click on a firewall policy.

Use this page to view and manage policy intents associated with your site or site groups. You can filter and sort this information to get a better understanding of what you want to configure.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a firewall policy intent. See [“Adding Firewall Policy Intents” on page 449](#).
- Modify, clone or delete firewall policy intents. See [“Editing, Cloning, and Deleting Firewall Policy Intents” on page 455](#).
- Deploy a firewall policy. See [“Deploying Policies” on page 742](#).

NOTE: An orange line is displayed against all undeployed firewall policy intents.

- Search for a firewall policy intent. Click the Search icon in the top right corner of the page to search for a firewall policy intent.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.
- View undeployed intents. Click the **Show Hide Columns** icon at the top right corner of the page and select **Undeployed Intent** under **Quick Filters**.

Field Descriptions

Table 113 on page 445 provides guidelines on using the fields on the **Firewall Policy** page.

Table 113: Fields on the Firewall Policy Page

Field	Description
Source	Source endpoint to which a firewall policy intent applies. A source endpoint can be addresses, sites, site groups, departments, users, or Internet (all in-bound traffic).
Destination	Destination endpoint to which a firewall policy intent applies. A destination endpoint can be addresses, services, sites, application signatures and groups, services and groups, or departments.
Options	Displays whether scheduling, logging, and UTM options are enabled for the firewall policy intent.
Total	Number of intents associated with the firewall policy.
Undeployed	Number of intents associated with the firewall policy that are either created new or updated, but are not yet deployed.

RELATED DOCUMENTATION

Firewall Policy Overview 441
Adding Firewall Policy Intents 449
Firewall Policy Examples 464
Editing, Cloning, and Deleting Firewall Policy Intents 455
About the Deployments Page 739
Deploying Policies 742

Adding a Firewall Policy

A firewall policy enforces rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall.

Use this page to add a firewall policy and assign it to one or more sites.

NOTE: A single policy can have both enterprise based intents and zone based intents for SD-WAN sites and next generation firewall sites.

To add a firewall policy:

1. Select **Configuration > Firewall > Firewall Policy**,
The Firewall Policy page appears.
2. Click the plus icon (+).
The Add Firewall Policy page appears.
3. Complete the configuration settings according to the guidelines provided in [Table 114 on page 446](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.
The new firewall policy is created and a confirmation message is displayed.

Table 114: Fields on the Add Firewall Policy Page

Field	Description
Name	Enter a unique string of alphanumeric characters that can include spaces and some special characters. The maximum length is 255 characters.
Description	Enter a description for the policy; the maximum length is 255 characters.
All Sites	Click the toggle button to apply the firewall policy to all sites.

Table 114: Fields on the Add Firewall Policy Page (continued)

Field	Description
Select Sites	<p>Applicable only if you have not enabled the All Sites toggle button.</p> <p>Select one or more sites or site groups to which the policy must be applied.</p> <p>Select the sites or site groups from the Available column and click the right-arrow to move the sites or site groups to the Selected column.</p> <p>If you add a site to (or remove a site from) a site group that is selected in a firewall policy, CSO marks the policy as Redeploy Required, and you need to manually redeploy that policy. If you activate a site belonging to a site group selected in a firewall policy that is in the Deployed state, the policy is automatically deployed to that site.</p>

Editing and Deleting Firewall Policies

IN THIS SECTION

- [Editing Firewall Policies | 448](#)
- [Deleting Firewall Policies | 448](#)

You can edit and delete firewall policies from the **Firewall Policy** page.

Editing Firewall Policies

NOTE: You cannot modify the firewall policy name.

To modify the parameters configured for a firewall policy:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the list of firewall policies.

2. Hover over the firewall policy that you want to edit, and then click the ... icon that appears on the right side of the page.

3. Click **Edit**.

The Edit Firewall Policy page appears displaying the same options that you entered while creating the firewall policy.

4. Modify the parameters following the guidelines provided in [“Adding a Firewall Policy” on page 445](#).

5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **Save**, the modified policy appears on the **Firewall Policy** page.

Deleting Firewall Policies

To delete a firewall policy:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the list of firewall policies.

2. Select the firewall policy that you want to delete and then click the ... icon that appears on the right side of the policy and click **Remove**.

Alternatively, you can select the firewall policy and click the Delete icon.

A message requesting confirmation for the deletion appears.

3. Click **Yes** to delete the selected firewall policy. If you want to discard your changes, click **Cancel** instead.

If you click **Yes**, the selected policy is deleted from the Firewall Policy page.

RELATED DOCUMENTATION

| [Adding a Firewall Policy](#) | 445

Adding Firewall Policy Intents

Use this page to add a firewall intent that controls transit traffic within a context. The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database.

You can also enable advanced security protection by specifying one or more of the following:

- Unified threat management (UTM) profile
- SSL proxy profile
- Intrusion prevention system (IPS) profile

To configure a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The Firewall Policy page appears.

2. Click the firewall policy to which you want to add the intent.

The *Firewall-Policy-Name* page appears.

3. Click the add icon (+).

The option to create firewall policy intent appears inline on the *Firewall-Policy-Name* page.

4. Complete the configuration according to the guidelines provided in [Table 115 on page 450](#).

5. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **Save**, a new firewall policy intent with the provided configuration is saved and a confirmation message is displayed. Based on the source and destination end points, the intents are categorized as zone-based intents and enterprise-based intents.

NOTE: After the policy intent is created, you must deploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications. When a firewall policy intent is created, the Undeployed field is incremented by one indicating that intents are pending deployment.

Table 115: Fields on the <Firewall-Policy-Name> Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters. If you do not enter a name, the intent is saved with a default name assigned by CSO.
Description	Enter a description for the policy intent; maximum length is 1024 characters.
Select Schedule	<p>Policy schedules enable you to define when a policy is active, and thus are an implicit match criterion. You can define the day of the week and the time of the day when the policy is active. For instance, you can define a security policy that opens or closes access based on business hours. Select a pre-saved schedule and the schedule options are populated with the selected schedule's data.</p> <p>You can add a schedule from the End Points panel, by selecting the schedule and clicking on the check mark icon (✓).</p> <p>You can also create new schedules and then associate the schedule to your firewall policy.</p> <p>To create a new schedule and then add it to a firewall policy:</p> <ol style="list-style-type: none"> 1. Click Select Schedule. 2. Click Add schedule. The Create Schedules page appears. 3. Create a new schedule. See “Creating Schedules” on page 506. The new schedule appears in the End Points tab, under Schedules. 4. Select the schedule and click on the add icon (+) to add it to the firewall policy.

Table 115: Fields on the <Firewall-Policy-Name> Page (continued)

Field	Description
Logging	<p>Click the toggle button to enable logging; by default, logging is disabled. You can see the logged firewall events in the Firewall Events page by using Monitor > Security Events > Firewall Events.</p> <p>For more information, see “About the Firewall Events Page” on page 828.</p>
<i>Identify the traffic that the intent applies to</i>	
Source	<p>Click the add icon (+) to select the source end points on which the firewall policy intent applies, from the displayed list of addresses, departments, sites, site groups, users, zones, or the Internet. You can also select a source end point using the methods described in “Selecting Firewall Source” on page 457.</p>
Destination	<p>Click the add icon (+) to select the destination end points on which the firewall policy intent applies, from the displayed list of addresses, applications, application groups, departments, services, sites, site groups, zones or the Internet. You can also select a destination end point using the methods described in “Selecting Firewall Destination” on page 461.</p>
Select Action	<p>Click the add icon (+) to choose whether you want to permit, deny, or reject traffic between the source and destination.</p> <ul style="list-style-type: none"> ● Allow—Device permits traffic using the type of firewall authentication you applied to the policy. ● Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. ● Reject—Device sends a TCP reset if the protocol is TCP, and device sends an ICMP reset if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources so that applications do not waste time waiting for timeouts and instead get the active message.

Table 115: Fields on the <Firewall-Policy-Name> Page (*continued*)

Field	Description
Advanced Security	<p>NOTE: This field is enabled only if you either select Allow for the action or if you select a zone as a source and destination.</p> <ul style="list-style-type: none"> UTM Profile—When you set the action to Allow, you can specify a UTM profile by selecting a profile from the list (under UTM Profiles [UTM]). You specify a UTM profile for protection against multiple threat types including spam and malware, and control access to unapproved websites and content. You can add a new UTM profile by clicking + in the End Points pane and selecting UTM Profiles. See “Creating UTM Profiles” on page 525. IPS Profile—When you set the action to Allow, you can specify an IPS profile by selecting a profile from the list (under IPS Profiles [IPS]). You specify an IPS profile to monitor and prevent intrusions. SSL Proxy Profile—When you configure a zone as part of the source and the destination, you can specify an SSL proxy profile by selecting a profile from the list (under SSL Profiles [SSLP]). You add an SSL proxy profile to ensure the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. You can also add a new SSL proxy profile by clicking + in the End Points pane and selecting SSL Proxy Profile. See “Creating SSL Forward Proxy Profiles” on page 729.
<i>Add source and destination end points</i>	

Table 115: Fields on the <Firewall-Policy-Name> Page (continued)

Field	Description
End Points	

Table 115: Fields on the <Firewall-Policy-Name> Page (continued)

Field	Description
	<p>To add an end point to the source or destination:</p> <ol style="list-style-type: none"> Click on Select Source or Select Destination text box and then click the lesser-than icon on the right side of the page to open the End Points panel. <p>The End Points panel displays the end points relevant to the source or destination based on your selection.</p> <ul style="list-style-type: none"> End points from addresses, departments, users, zones, and sites are displayed for source. <p>NOTE: If JIMS is not configured for CSO, users will not be listed in the End Points panel. Instead you will be provided with an option to import users through the Administration > Identity Management page. To import users, click Set Up and follow the steps provided in "About the Identity Management Page" on page 433.</p> <ul style="list-style-type: none"> End points from addresses, applications, departments, services, zones, and sites are displayed for destination. <p>NOTE: You can also search for a specific end point using the search option.</p> <ol style="list-style-type: none"> (Optional) Click on the edit icon (pencil symbol) to modify an end point. (Optional) Click on the details icon on the right of the end point, to view more information about a source or destination end point. Select the end point you want to add and click on the check mark icon (✓) to add it the source or destination. <p>The selected end point is added to the source or destination.</p> <p>To add new source and destination end points:</p> <ol style="list-style-type: none"> Click the less-than icon (<) on the right side of the page, to open the End Points panel. Click on the add icon (+) on the top right of the End Points panel. <p>A list of end points that you can add is displayed.</p> <ol style="list-style-type: none"> Select the end point you want to add. <p>You can add the following end points:</p> <ul style="list-style-type: none"> Address or address group. See "Creating Addresses or Address Groups" on

Table 115: Fields on the <Firewall-Policy-Name> Page (continued)

Field	Description
	<p>page 753.</p> <ul style="list-style-type: none">• Site or site group. See “Creating Site Groups” on page 217.• Department. See “Add a Department” on page 783.• Service or service group. See “Creating Services and Service Groups” on page 759.• Application signature or application signature group. See “Adding Application Signatures” on page 772, and “Adding Application Signature Groups” on page 779.• Create a schedule. See “Creating Schedules” on page 506. <p>4. Click Save to add the new end point.</p> <p>The created end point is listed in the End Points panel.</p> <p>5. Select the end point you want to add to the source or destination, and click on the check mark icon (✓).</p> <p>The end point is added to the source or destination.</p>

RELATED DOCUMENTATION

Firewall Policy Overview	441
About the Firewall Policy Name Page	444
Firewall Policy Examples	464
Editing, Cloning, and Deleting Firewall Policy Intents	455

Editing, Cloning, and Deleting Firewall Policy Intents

IN THIS SECTION

- Editing Firewall Policy Intents | 456
- Cloning Firewall Policy Intents | 456
- Deleting Firewall Policy Intents | 457

You can edit, clone, and delete firewall policy intents from the **Firewall Policy** page.

Editing Firewall Policy Intents

To modify the parameters configured for a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the list of firewall policies.

2. Click the firewall policy for which you want to edit the firewall policy intents.

The firewall policy intents are displayed in the Firewall Policy page.

3. Hover over the firewall policy intent that you want to edit, and then click the ... icon that appears on the right side of the intent. Click **Edit**.

The **Firewall Policy** page displays the same options as those that appear when you create a new firewall policy intent.

4. Modify the parameters following the guidelines provided in [“Adding Firewall Policy Intents” on page 449](#).

5. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **Save**, the modified intent appears on the **Firewall Policy** page.

Cloning Firewall Policy Intents

To clone a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the intents associated with the policy.

2. Click the firewall policy for which you want to clone the firewall policy intents.

The firewall policy intents are displayed in the Firewall Policy page.

3. Hover over the firewall policy intent that you want to clone, and then click the ... icon that appears on the right side of the intent. Click **Clone**.

The **Firewall Policy** page displays the same options as those that appear when you create a new firewall policy intent. Update the cloned intent as required.

4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **Save**, the cloned intent is added to the firewall policy and appears on the **Firewall Policy** page.

Deleting Firewall Policy Intents

To delete a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the intents associated with the policy.

2. Click the firewall policy for which you want to delete the firewall policy intent.

The firewall policy intents are displayed in the Firewall Policy page.

3. Select the firewall policy intent you want to delete, and then click the ... icon that appears on the right side of the intent. Click **Delete**.

An alert message appears, verifying that you want to delete the selected intent.

4. Click **Yes** to delete the selected intent. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected intent is deleted from the policy.

RELATED DOCUMENTATION

[Firewall Policy Overview | 441](#)

[About the Firewall Policy Name Page | 444](#)

[Firewall Policy Examples | 464](#)

[Adding Firewall Policy Intents | 449](#)

Selecting Firewall Source

IN THIS SECTION

- [Adding an End Point as Firewall Source | 458](#)
- [Selecting Firewall Source Using Abbreviations | 459](#)
- [Selecting a Firewall Source from the End Points Panel | 459](#)

- Creating and Selecting a Firewall Source from the End Points Panel | 460
- Creating Addresses from Source | 460

The following procedures provides various methods using which you can choose a firewall source end point:

Adding an End Point as Firewall Source

View and select the source end point from the complete list of addresses, sites, site groups, zones, or departments. You can also select the **Internet** option which denotes all in-coming traffic from outside your network.

NOTE: When you select **Any** address as a source, it implies traffic originating within the network.

NOTE:

The following conditions apply when you select **Internet** as a source end point:

- When **Internet** is not chosen as a source end point, it is implied that the traffic is originating within the network.
- If you chose **Internet** as a source, you cannot add other sites, site groups or departments as a source end point along with **Internet**.
- If you chose **Internet** as a source, the destination end point must be a site, site group, or department.

1. Click the **Source** field. A list of relevant endpoints are displayed.
2. Click on **View more results** link provided at the bottom of the source end points. The complete list of addresses, departments, users, sites, site groups, and zones is displayed in the **End Points** panel on the right.
3. (Optional) Click the edit icon to edit the address, users, department, or site group end point. You cannot edit a site end point.
4. Click check mark icon (✓) to select the end point as a source.

Selecting Firewall Source Using Abbreviations

Enter an abbreviation in the **Source** field to select the source end point from a filtered list of source endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of departments, enter **DEPT** or **dept**.
- To view a filtered list of sites, enter **SITE** or **site**.
- To view a filtered list of site groups, enter **STGP** or **stgp**.
- To view a filtered list of user ids, enter **USER** or **user**.
- To view a filtered list of zones, enter **ZONE** or **zone**.

Click the endpoints in the filtered list to select them. You can also select the end point from the complete list of addresses, departments, users, sites, and site groups. See [“Adding an End Point as Firewall Source” on page 458](#).

Selecting a Firewall Source from the End Points Panel

You can select a firewall source end point from the **End Points** panel. Alternately, you can create a new firewall source end point from the **End Points** panel, see [“Creating and Selecting a Firewall Source from the End Points Panel” on page 460](#)

To select an firewall source end point from the from the **End Points** panel:

1. Click on the **Source** field.
2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, departments, users, sites, site groups, and zones.

3. (Optional) To view more information about a source end point, click the details icon on the right of the end point. To edit the source end point, click the edit icon (pencil symbol) on the right of the end point.

NOTE: You can only edit or view details of a source end point if these options appear on right side of the end point when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the end point as a source.

Creating and Selecting a Firewall Source from the End Points Panel

To create a new source end point from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of end point you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to create a new end point.

- To create a new address, see [“Creating Addresses or Address Groups” on page 753](#).
- To create a site or site group, see [“Creating Site Groups” on page 217](#).

After the end point is created, it appears in the **End Points** panel.

2. Click the check mark icon (✓) to add the new end point as a source.

Creating Addresses from Source

You can use one of the following ways to create a new address from the **Source** field and use the newly created address as a source end point:

- Type the address directly in the **Source** field. If the address is valid, it is created immediately and added as a source end point.
- Create an address from the **Source** field, using the following steps:

1. In the **Source** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.
2. Click **Add new address** to create a new address.

The **Create Addresses** page appears.

3. Configure the new address. See [“Creating Addresses or Address Groups” on page 753](#).
4. Click **Save** to save the new address.

The new address is created, and will be listed as an option for the source. Select the new address to add it to the source.

RELATED DOCUMENTATION

[Selecting Firewall Destination | 461](#)

[Adding Firewall Policy Intents | 449](#)

[Firewall Policy Overview | 441](#)

[About the Firewall Policy Name Page | 444](#)

[Editing, Cloning, and Deleting Firewall Policy Intents | 455](#)

Selecting Firewall Destination

IN THIS SECTION

- [Adding an End Point as Firewall Destination | 461](#)
- [Selecting Firewall Destination Using Abbreviations | 462](#)
- [Selecting a Firewall Destination from the End Points Panel | 462](#)
- [Creating and Selecting a Firewall Destination from the End Points Panel | 463](#)
- [Creating Addresses from Destination | 463](#)

The following procedures provides various methods using which you can choose a firewall destination end point:

Adding an End Point as Firewall Destination

View and select the end point from the complete list of addresses, applications, application groups, departments, services, sites, site groups, or zones.

NOTE:

- When you choose **Any** address or service as the destination, it implies that traffic is flowing outside the network unless a site or department is mentioned explicitly.
- Unless you choose a site, site group, or department as a destination end point, it is implied the traffic will flow outside your network.

1. Click on **Destination**. A list of relevant end points are displayed.
2. Click on **View more results** link provided at the bottom of the destination end points. The complete list of addresses, departments, sites, and site groups is displayed in the **End Points** panel on the right.

3. (Optional) Click the edit icon to edit the address, department, or site group end point. You cannot edit a site end point.
4. Click check mark icon (✓) to select the end point as a destination.

Selecting Firewall Destination Using Abbreviations

Enter an abbreviation in the **Destination** field to select the destination end point from a filtered list of destination endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of applications or application groups, enter **APPS** or **apps**.
- To view a filtered list of departments, enter **DEPT** or **dept**.
- To view a filtered list of services, enter **SVCS** or **svcs**.
- To view a filtered list of sites, enter **SITE** or **site**.
- To view a filtered list of site groups, enter **STGP** or **stgp**.
- To view a filtered list of zones, enter **ZONE** or **zone**.

Click the endpoints in the filtered list to select them. You can also select the end point from the complete list of addresses, departments, sites, and site groups. See [“Adding an End Point as Firewall Destination” on page 461](#).

Selecting a Firewall Destination from the End Points Panel

You can select a firewall destination end point from the **End Points** panel. Alternately, you can create a new firewall destination end point from the **End Points** panel, see [“Creating and Selecting a Firewall Destination from the End Points Panel” on page 463](#).

To select an firewall destination end point from the from the **End Points** panel:

1. Click on the **Destination** field.
2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, applications, application groups, departments, services, sites, site groups, or zones.

3. (Optional) To view more information about a destination end point, click the details icon on the right of the end point. To edit the destination end point, click the edit icon (pencil symbol) on the right of the end point.

NOTE: You can only edit or view details of a destination end point if these options appear on right side of the end point when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the end point as a destination.

Creating and Selecting a Firewall Destination from the End Points Panel

To create an new destination end point from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of end point you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to add a new end point.

- To add a new address, see [“Creating Addresses or Address Groups” on page 753](#).
- To add a site or site group department, see [“Creating Site Groups” on page 217](#).
- To add an application or application group, see [“Adding Application Signatures” on page 772](#) and [“Adding Application Signature Groups” on page 779](#).
- To add a new service, see [“Creating Services and Service Groups” on page 759](#).
- To add an SSL proxy profile, see [“Creating SSL Forward Proxy Profiles” on page 729](#).
- To add an UTM Profile, see [“Creating UTM Profiles” on page 525](#).

After the end point is created, it appears in the **Endpoints** panel.

2. Click the check mark icon (✓) to add the new end point as a destination.

Creating Addresses from Destination

You can use one of the following ways to create a new address from the **Destination** and use the newly created address as a destination end point:

- Type the address directly in the **Destination** field. If the address is valid, it is created immediately and added as a destination end point.

- Create an address from the **Destination** field, using the following steps:
 1. In the **Destination** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.
 2. Click **Add new address** to create a new address.
The **Create Addresses** page appears.
 3. Configure the new address. See [“Creating Addresses or Address Groups” on page 753](#).
 4. Click **Save** to save the new address.
The new address is created, and will be listed as an option for the destination. Select the new address to add it to the destination.

RELATED DOCUMENTATION

[Adding Firewall Policy Intents | 449](#)

[Firewall Policy Overview | 441](#)

[About the Firewall Policy Name Page | 444](#)

[Editing, Cloning, and Deleting Firewall Policy Intents | 455](#)

Firewall Policy Examples

IN THIS SECTION

- [Example 1: Firewall Policy that Permits Traffic from Departments in Site A to the Departments in Site B | 466](#)
- [Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B | 468](#)
- [Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B | 471](#)
- [Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A | 472](#)
- [Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments | 474](#)
- [Example 6: Firewall Policy that Denies Access to Social Networking Sites | 482](#)
- [Example 7: Firewall Policy that Controls Access to an Address over the Internet \(HTTP\) | 485](#)
- [Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service | 491](#)

- Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B | 493
- Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A | 496
- Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled | 500
- Example 12: Firewall Policy that blocks access to Internet and allow access to Google Drive. | 503

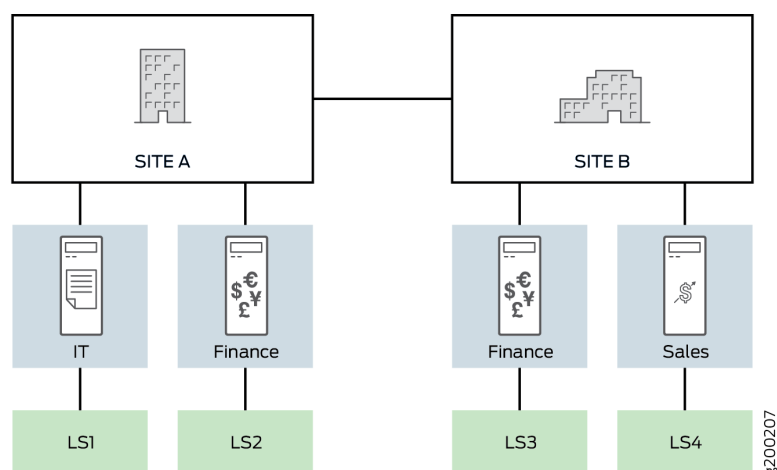
This topic provides information on how firewall policy intents that you define as part of your firewall policy is handled by Contrail Service Orchestration (CSO), using various examples. Each of the examples provide detailed explanation about how a firewall policy intent defined through the CSO GUI resolves into configuration in the system.

NOTE: For more information, see [“Firewall Policy Overview” on page 441](#) and [“Adding Firewall Policy Intents” on page 449](#).

For easier understanding, all the examples have been defined to use the topology in illustrated in [Figure 19 on page 465](#). In this topology, there are two sites—site A and site B. Each site has two departments defined as follows:

- Site A - IT (LAN segment LS1) and Finance (LAN segment LS2).
- Site B - Finance (LAN segment LS3) and Sales (LAN segment LS4).

Figure 19: Topology Diagram



The following definitions are applicable to all the examples:

- While creating a site, you can designate some of the WAN interfaces to be breakout interfaces. These WAN interfaces can carry both site-to-site traffic (through the trust zone) and breakout traffic (through the untrust zone). The WAN interfaces can also be designated exclusively for carrying breakout traffic.
- A trust zone refers to the overlay interface that contains all the GRE tunnel interfaces, such as gr-0/0/0.1, gr-0/0/0.2, and IPsec interfaces, such as st0.1, st0.2 created between the sites.
- An untrust zone refers to the underlay interfaces (underlying physical interfaces) such as ge-0/0/0, ge-0/0/1.
- If you select an address or a service as a destination endpoint, CSO considers it as an address or service hosted on the Internet, unless the selected address or service is associated with a site.
- [Table 116 on page 466](#) captures the addresses associated with the LAN segments used in the topology illustrated in [Figure 19 on page 465](#).

Table 116: LAN Segments Definition

Site	Department	LAN Segment	LAN Segment Address
site A	IT	LS1	192.0.2.0/24
site A	Finance	LS2	192.168.1.0/24
site B	Finance	LS3	198.51.100.0/24
site B	Sales	LS4	203.0.113.0/24

The following examples help you understand the creation of intent-based firewall policies for various traffic scenarios across sources and destinations.

Example 1: Firewall Policy that Permits Traffic from Departments in Site A to the Departments in Site B

Define a firewall policy that permits traffic from the departments in site A to the departments in site B.

[Table 117 on page 466](#) shows the firewall policy intent that is defined:

Table 117: Firewall Policy Intent Definition for Example - 1

Source	Destination	Action
site A	site B	Permit

[Table 118 on page 467](#) shows how this firewall policy intent is resolved:

Table 118: Firewall Policy Intent Resolution for Example - 1

Site	Source Department	Source Address	Zone	Destination Address	Service	Intent Created
site A	Finance	[LS2]	Trust	[LS3, LS4]	Any	Intent 1__0
	IT	[LS1]	Trust	[LS3, LS4]	Any	Intent 1__1
site B	Trust	[LS3, LS4]	Sales	[LS2]	Any	Intent 1__0
	Trust	[LS3, LS4]	Finance	[LS1]	Any	Intent 1__1

Configuration Output Sample

Sample of configuration that permits traffic from departments in site A to the departments in site B.

The hierarchy level for the following configuration sample is [\[edit security policies\]](#).

```

from-zone FINANCE to-zone trust {
  policy Intent_1__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address [ls-198.51.100.0/24-SP50-L3,
ls-203.0.113.0/24-SP50-L4];
      application any;
    }
    then {
      permit;
    }
  }
}

from-zone IT to-zone trust {
  policy Intent_1__1 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address [ls-198.51.100.0/24-SP50-L3,
ls-203.0.113.0/24-SP50-L4];
      application any;
    }
    then {
      permit;
    }
  }
}

```

```

    }
  }
}

```

Sample of configuration that permits traffic from departments in site B to the departments in site A.

The hierarchy level for the following configuration sample is [\[edit security policies\]](#).

```

from-zone trust to-zone SALES {
  policy Intent_1__0 {
    match {
      source-address [ls-198.51.100.0/24-SP50-L3,
        ls-203.0.113.0/24-SP50-L4];
      destination-address ls-192.0.2.0/24-S42-L1;
      application any;
    }
    then {
      permit;
    }
  }
}

from-zone trust to-zone FINANCE {
  policy Intent_1__1 {
    match {
      source-address [ls-198.51.100.0/24-SP50-L3,
        ls-203.0.113.0/24-SP50-L4];
      destination-address ls-192.168.1.0/24-SP50-L2;
      application any;
    }
    then {
      permit;
    }
  }
}

```

Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B

Define a firewall policy that permits all the department in site A and site B access to Internet.

[Table 119 on page 469](#) shows the firewall policy intent that is defined:

Table 119: Firewall Policy Intent Definition for Example - 2

Source	Destination	Action
site A	http, https, icmp-ping, dns	Permit
site B	http, https, icmp-ping, dns	Permit

Table 120 on page 469 shows how this firewall policy intent is resolved:

Table 120: Firewall Policy Intent Resolution for Example - 2

Site	Source Department	Source Address	Zone	Destination Address	Service	Intent Created
site A	Finance	[LS2]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__0
	IT	[LSI]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__1
site B	Sales	[LS4]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__0
	Finance	[LS3]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__1

Configuration Output Sample

Sample of configuration that permits Internet access to all departments in site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_1__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
    }
  }
}

```

```

        application [junos-http junos-dns-tcp junos-https
                    junos-icmp-ping];
    }
    then {
        permit;
    }
}
}
from-zone IT to-zone untrust {
    policy Intent_1__1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address any;
            application [junos-http junos-dns-tcp junos-https
                    junos-icmp-ping];
        }
        then {
            permit;
        }
    }
}
policy-rematch;

```

Sample of configuration that permits Internet access to all departments in site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Sales to-zone untrust {
    policy Intent_1__0 {
        match {
            source-address ls-203.0.113.0/24-SP50-L4;
            destination-address any;
            application [junos-http junos-dns-tcp junos-https
                    junos-icmp-ping];
        }
        then {
            permit;
        }
    }
}
from-zone Finance1 to-zone untrust {

```

```

policy Intent_1__1 {
  match {
    source-address ls-198.51.100.0/24-SP50-L3;
    destination-address any;
    application [junos-http junos-dns-tcp junos-https
               junos-icmp-ping];
  }
  then {
    permit;
  }
}
policy-rematch;

```

Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B

Define a firewall policy that permits any public Internet address access to a sales application hosted by the Sales department in site B.

NOTE: For this example, breakout is not enabled and MPLS link type is used.

Table 121 on page 471 shows the firewall policy intent that is defined:

Table 121: Firewall Policy Intent Definition for Example - 3

Source	Destination	Action
Internet	Sales, site B	Permit

Table 122 on page 471 shows how this firewall policy intent is resolved:

Table 122: Firewall Policy Intent Resolution for Example - 3

Source Address	Zone	Destination Address	Service	Intent Created
Any public Internet address	Trust to Sales (No breakout)	[LS4]	Any	Intent 1__0

Configuration Output Example

Sample of configuration that permits any public Internet address to access the Sales department in site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone untrust to-zone Sales {
  policy Intent_1__0 {
    match {
      source-address any;
      destination-address ls-203.0.113.0/24-SP50-L4;
      application any;
    }
    then {
      permit;
    }
  }
}

```

Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A

Define a firewall policy that permits all departments in site A access to Facebook.

[Table 123 on page 472](#) shows the firewall policy intent that is defined:

Table 123: Firewall Policy Intent Definition for Example - 4

Source	Destination	Action
site A	Facebook	Permit

[Table 124 on page 472](#) shows how this firewall policy intent is resolved:

Table 124: Firewall Policy Intent Resolution for Example - 4

Site	Source Address	Zone	Destination Address	Service	Intent Created	Application Firewall Profile
site A	[LS2]	Untrust	Facebook	Any	Intent 1__0	AppFwProfile_0
site A	[LS1]	Untrust	Facebook	Any	Intent 1__1	AppFwProfile_0

Configuration Output Example

Sample of configuration that controls access to Facebook for site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_1__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

from-zone IT to-zone untrust {
  policy Intent_1__1 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

policy-rematch;
```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

application-firewall {
  rule-sets AppFwProfile_0 {
    rule rule-1 {
      match {
        dynamic-application junos:FACEBOOK-APP;
        ssl-encryption any;
      }
      then {
        permit;
      }
    }
    default-rule {
      deny;
    }
  }
}

```

Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments

Define a firewall policy that controls access to specific applications from various departments, with the following intents:

- The finance departments located in site A and site B (which are in different geographical locations) are permitted to access the news applications BBC and CNN.
- The IT department located in site A is denied access to the news applications BBC and CNN.
- Access to Telnet and SSH applications is given only to the finance departments.
- Access to Telnet and SSH applications is denied to all departments, except for the finance department.

[Table 125 on page 474](#) shows the firewall policy intents that are to fulfil this requirement:

Table 125: Firewall Policy Intent Definition for Example - 5

Source	Destination	Action
Finance department, site A and Finance department, site B	BBC and CNN	Permit
IT department, site A	BBC and CNN	Deny
Finance department, site A and Finance department, site B	Telnet and SSH	Permit

Table 125: Firewall Policy Intent Definition for Example - 5 (continued)

Source	Destination	Action
Any (All addresses except the finance department)	Telnet and SSH	Deny

NOTE: The number of intents depends on the number of source sites within the given department and the number of destination sites.

Table 126 on page 475 shows how this firewall policy intent is resolved:

Table 126: Firewall Policy Intent Resolution for Example - 5

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
Finance	[LS2]	Trust/Untrust	Any	Any	AppFwProfile_1 Permit: CNN/BBC Def. Rule : Permit
Finance	[LS3]	Trust/Untrust	Any	Any	AppFwProfile_1 Permit: CNN/BBC Def. Rule : Permit
IT	[LS1]	Trust/Untrust	Any	Any	AppFwProfile_3 Deny: CNN/BBC Def. Rule : Deny
Finance department, site A and Finance department, site B	[LS2, LS3]	Trust/Untrust	Any	Telnet, SSH	AppFwProfile_1-1 Permit: Telnet/SSH Def. Rule : Deny

Table 126: Firewall Policy Intent Resolution for Example - 5 (continued)

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
IT department, site A	[LS1]	Trust/Untrust	Any	Telnet, SSH	AppFwProfile_3-1 Deny: Telnet/SSH Def. Rule : Deny

Configuration Output Example

Sample of configuration that controls access to specific applications for various departments in site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone trust {
  policy Intent_3 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application [junos-telnet junos-ssh];
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1-1;
          }
        }
      }
    }
  }
}
policy Intent_1 {
  match {
    source-address ls-192.168.1.0/24-SP50-L2;
    destination-address any;
    application any;
  }
  then {
    permit {

```

```

        application-services {
            application-firewall {
                rule-set AppFwProfile_1;
            }
        }
    }
}
policy Intent_4__0 {
    match {
        source-address any;
        destination-address any;
        application [junos-telnet junos-ssh];
    }
    then {
        permit;
    }
}
from-zone IT to-zone trust {
    policy Intent_4__1-1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address any;
            application [junos-telnet junos-ssh];
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_3-1;
                    }
                }
            }
        }
    }
}
policy Intent_2 {
    match {
        source-address ls-192.0.2.0/24-S42-L1;
        destination-address any;
        application any;
    }
}

```

```

        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_3;
                    }
                }
            }
        }
    }
}
policy Intent_4__1 {
    match {
        source-address any;
        destination-address any;
        application [junos-telnet junos-ssh];
    }
    then {
        deny;
    }
}
}

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_1-1 {
    rule rule-1 {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}
rule-sets AppFwProfile_3 {
    rule rule-2 {

```

```

        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

rule-sets AppFwProfile_1 {
    rule rule-3 {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}

rule-sets AppFwProfile_3-1 {
    rule rule-4 {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

```

Sample of configuration that controls access to specific applications for various departments in site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone trust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
  policy Intent_3 {
    match {
      source-address ls-198.51.100.0/24-SP50-L3;
      destination-address any;
      application [ junos-telnet junos-ssh ];
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1-1;
          }
        }
      }
    }
  }
  policy Intent_1 {
    match {
      source-address ls-198.51.100.0/24-SP50-L3;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1;
          }
        }
      }
    }
  }
}

```

```

        }
    }
}
policy Intent_4__1 {
    match {
        source-address any;
        destination-address any;
        application [junos-telnet junos-ssh];
    }
    then {
        deny;
    }
}
}
from-zone Sales to-zone trust {
    policy Intent_4__0 {
        match {
            source-address any;
            destination-address any;
            application [junos-telnet junos-ssh];
        }
        then {
            deny;
        }
    }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_1-1 {
    rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}

```

```
    }
rule-sets AppFwProfile_1 {
  rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
    match {
      dynamic-application [junos:BBC junos:CNN];
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}
```

Example 6: Firewall Policy that Denies Access to Social Networking Sites

Define a firewall policy that denies access to networking sites such as Facebook and Twitter (defined as application group Social Networking) to the IT and finance departments located in Site A.

Table 127 on page 482 shows the firewall policy intent that is needed to fulfil this requirement:

Table 127: Firewall Policy Intent Definition for Example - 6

Source	Destination	Action
IT and Finance, site A	Application group Social Networking (Facebook and Twitter)	Deny

NOTE: Add site A if the IT or finance departments are present in different sites, but you only want to apply this firewall policy intent to the IT or finance departments present in site A.

Table 128 on page 483 shows how this firewall policy intent is resolved:

Table 128: Firewall Policy Intent Resolution for Example - 6

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
Finance	[LS2]	Trust/Untrust	Any	Any	AppFwProfile_0 Deny: Social Networking (Apps) Def. Rule : Deny
IT	[LS1]	Trust/Untrust	Any	Any	AppFwProfile_1 Deny: Social Networking (Apps) Def. Rule : Deny

Configuration Output Example

Sample of configuration that denies access to social networking sites for departments in site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone IT to-zone untrust {
  policy Intent_1__0 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

```

```

    }
  }
  from-zone Finance to-zone untrust {
    policy Intent_1__1 {
      match {
        source-address ls-192.168.1.0/24-SP50-L2;
        destination-address any;
        application any;
      }
      then {
        permit {
          application-services {
            application-firewall {
              rule-set AppFwProfile_0;
            }
          }
        }
      }
    }
  }
}

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

application-firewall {
  rule-sets AppFwProfile_0 {
    rule rule-b7e4ed02-e196-400a-88bf-f1de8973d30c-appFwRule {
      match {
        dynamic-application-group Socialnetwork;
        ssl-encryption any;
      }
      then {
        deny;
      }
    }
    default-rule {
      deny;
    }
  }
}

```

}

Example 7: Firewall Policy that Controls Access to an Address over the Internet (HTTP)

Define a firewall policy that controls access to an address over the Internet (HTTP) for various sites or site groups with the following intents:

- IP address prefix of site A and site B are permitted to access example.com.
- IP address prefix of site group Q1 are denied access to example-one.com. Site group Q1 consists of site A and site B.

Table 129 on page 485 shows the firewall policy intents that are needed to fulfil this requirement:

Table 129: Firewall Policy Intent Definition for Example - 7

Source	Service	Destination	Action
IP address prefix, site A and IP-Prefix, site B	HTTP	www.example.com	Permit
IP address prefix, site group Q1	HTTP	www.example-one.com	Deny

Table 130 on page 485 shows how this firewall policy intent is resolved:

Table 130: Firewall Policy Intent Resolution for Example - 7

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
IT, Finance departments in site A	[LS1, LS2]	Trust/Untrust	www.example.com	Any	AppFwProfile_0 Permit: HTTP Def. Rule : Deny
Finance, Sales departments in site B	[LS3, LS4]	Trust/Untrust	www.example.com	Any	AppFwProfile_1 Permit: HTTP Def. Rule : Deny

Table 130: Firewall Policy Intent Resolution for Example - 7 (continued)

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
IT, Finance departments in site A	[LS1, LS2]	Trust/Untrust	www.example-one.com	Any	AppFwProfile_2 Deny: HTTP Def. Rule : Deny
Finance, Sales departments in site B	[LS3, LS4]	Trust/Untrust	www.example-one.com	Any	AppFwProfile_3 Deny: HTTP Def. Rule : Deny

Configuration Output Example

Sample of configuration that controls access to an address over the Internet (HTTP) for site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_4__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address www.example.com;
      application junos-http;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}
policy Intent_1__0 {
  match {
    source-address ls-192.168.1.0/24-SP50-L2;

```

```

        destination-address addr2;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set AppFwProfile_1;
                }
            }
        }
    }
}

from-zone IT to-zone untrust {
    policy Intent_4__1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address addr2;
            application junos-http;
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_0;
                    }
                }
            }
        }
    }
}

policy Intent_1__1 {
    match {
        source-address ls-192.0.2.0/24-S42-L1;
        destination-address addr2;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set AppFwProfile_1;
                }
            }
        }
    }
}

```



```

        deny;
    }
}
default-rule {
    deny;
}
}

```

Sample of configuration that controls access to an address over the Internet (HTTP) for site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
    policy Intent_4__1 {
        match {
            source-address ls-198.51.100.0/24-SP50-L3;
            destination-address addr2;
            application junos-http;
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_0;
                    }
                }
            }
        }
    }
}
policy Intent_1__1 {
    match {
        source-address ls-198.51.100.0/24-SP50-L3;
        destination-address addr2;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set AppFwProfile_1;
                }
            }
        }
    }
}

```

```

    }
  }
}
from-zone Sales to-zone untrust {
  policy Intent_4__0 {
    match {
      source-address ls-203.0.113.0/24-SP50-L4;
      destination-address addr2;
      application junos-http;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
  policy Intent_1__0 {
    match {
      source-address ls-203.0.113.0/24-SP50-L4;
      destination-address addr2;
      application junos-http;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1;
          }
        }
      }
    }
  }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_1 {
  rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {

```



```

        match {
            dynamic-application junos:YOUTUBE;
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

rule-sets AppFwProfile_0 {
    rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bff38-appFwRule {
        match {
            dynamic-application junos:CNN;
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
        match {
            dynamic-application junos:YOUTUBE;
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

```

Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service

Define a firewall policy where a specific IP address that belongs to the IT department is permitted or denied the use of HTTP or FTP as a service.

[Table 131 on page 492](#) shows the firewall policy intents that are needed to fulfil this requirement:

Table 131: Firewall Policy Intent Definition for Example - 8

Source	Service	Destination	Action
192.0.2.0	HTTP	example.com	Permit
192.0.2.0	FTP	example.com	Deny

Table 132 on page 492 shows how this firewall policy intent is resolved:

Table 132: Firewall Policy Intent Resolution for Example - 8

Source Department	Source Address	Zone	Destination Address	Service
IT, site A	192.0.2.0	Trust/Untrust	example.com	FTP
IT, site A	192.0.2.0	Trust/Untrust	example.com	HTTP

Configuration Output Example

Sample of configuration that allows access to HTTP

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone IT to-zone trust {
  policy Intent_1__1 {
    match {
      source-address 192.0.2.0;
      destination-address example.com;
      application junos-ftp;
    }
    then {
      deny;
    }
  }
}
policy Intent_4__1 {
  match {
    source-address 192.0.2.0;
    destination-address example.com;
    application junos-http;
  }
}

```

```

        then {
            permit;
        }
    }
}
policy-rematch;

```

Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B

Define a firewall policy that denies access to BitTorrent for the Finance departments in site A and Site B.

Table 133 on page 493 shows the firewall policy intents that are needed to fulfil this requirement:

Table 133: Firewall Policy Intent Definition for Example - 9

Source	Destination	Action
site A, Finance department	BitTorrent	Deny
site B, Finance department	BitTorrent	Deny

Table 134 on page 493 shows how this firewall policy intent is resolved:

Table 134: Firewall Policy Intent Resolution for Example - 9

Site	Source Address	Zone	Destination Application	Service	Application Firewall Profile
Finance department, site A	[LS2]	Trust/Untrust	BitTorrent	Any	AppFwProfile_0 Deny: BitTorrent Def. Rule : Deny
Finance department, site B	[LS3]	Trust/Untrust	BitTorrent	Any	AppFwProfile_0 Deny: BitTorrent Def. Rule : Deny

Configuration Output Example

Sample of configuration that allows site A access to BitTorrent.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
  policy Intent_1 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
      log {
        session-init;
        session-close;
      }
    }
  }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```
rule-sets AppFwProfile_0 {
  rule rule-2226740d-03a9-483c-b315-eddc9ae8619a-appFwRule {
    match {
      dynamic-application junos:BITTORRENT;
      ssl-encryption any;
    }
    then {
      deny;
    }
  }
  default-rule {
    deny;
  }
}
```

Sample of configuration that allows site B to access to BitTorrent.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```
from-zone Financel to-zone untrust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
  policy Intent_4 {
    match {
      source-address ls-198.51.100.0/24-SP50-L3;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
```

```

        rule-set AppFwProfile_0;
    }
}
}
log {
    session-init;
    session-close;
}
}
}
}
policy-rematch;
```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_0 {
    rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bff38-appFwRule {
        match {
            dynamic-application junos:BITTORRENT;
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}
```

Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A

Define a firewall policy where the users that are a part of user group A are provided access only to Facebook, and no other applications. User group A consists of users located in site A.

[Table 135 on page 496](#) shows the firewall policy intent that is needed to fulfil this requirement:

Table 135: Firewall Policy Intent Definition for Example - 10

Source	Destination	Action
user group A, site A	Facebook	Permit

Table 136 on page 497 shows how this firewall policy intent is resolved:

Table 136: Firewall Policy Intent Resolution for Example - 10

Site	User/User Group	Source Address Range	Destination Address	Application
site A	user group A	192.0.2.0 to 192.0.2.20	Any	Facebook

Configuration Output Example

Sample of configuration that allows users in user group A access to Facebook.

The hierarchy level for the following configuration sample is [\[edit security policies\]](#).

```

from-zone Finance to-zone untrust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
}
policy Intent_4__0 {
  match {
    source-address ls-192.168.1.0/24-SP50-L2;
    destination-address any;
    application any;
    source-identity "USERFW.LOCAL\Cert Publishers";
  }
  then {
    permit {
      application-services {
        application-firewall {
          rule-set AppFwProfile_0;
        }
      }
    }
  }
}

```

```

        log {
            session-init;
            session-close;
        }
    }
}

from-zone IT to-zone untrust {
    policy appQoe-36600-Permit-rule {
        match {
            source-address any;
            destination-address any;
            application appQoe-36000;
        }
        then {
            permit;
        }
    }
    policy Intent_4__1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address any;
            application any;
            source-identity "USERFW.LOCAL\Cert Publishers";
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_0;
                    }
                }
            }
            log {
                session-init;
                session-close;
            }
        }
    }
}

policy-rematch;

```


The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```
rule-sets AppFwProfile_0 {
  rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bff38-appFwRule {
    match {
      dynamic-application junos:FACEBOOK-APP;
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}
```

The hierarchy level for the following configuration sample is **[edit services user-identification identity-management]**.

```
connection {
  connect-method https;
  port 443;
  primary {
    address 10.213.50.50;
    client-id 1234;
    client-secret "$ABC123"; ## SECRET-DATA
  }
  token-api oauth_token/oauth;
  query-api user_query/v2;
}
batch-query {
  items-per-batch 200;
  query-interval 5;
}
ip-query {
  query-delay-time 15;
}
```

Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled

Define a firewall policy where the User B located in Site A is provided access only to YouTube with UTM enabled. The user does not have permission to access any other applications.

Table 137 on page 500 shows the firewall policy intent that is needed to fulfil this requirement:

Table 137: Firewall Policy Intent Definition for Example - 11

Source	Destination	Action
user B, site A	YouTube	Permit

Table 138 on page 500 shows how this firewall policy intent is resolved:

Table 138: Firewall Policy Intent Resolution for Example - 11

Site	Source Address	User/User Group	Destination Address	UTM	Application
site A	192.0.2.22	user B	Any	Enabled	Facebook

Configuration Output Example

Sample of configuration that allows user B in site A access to YouTube, with UTM enabled.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_4__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application any;
      source-identity "userfw.local\CS01";
    }
    then {
      permit {
        application-services {
          utm-policy testUTM;
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

```

```

    }
  }
  log {
    session-init;
    session-close;
  }
}
}
}
}
from-zone IT to-zone untrust {
  policy Intent_4__1 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address any;
      application any;
      source-identity "userfw.local\CS01";
    }
    then {
      permit {
        application-services {
          utm-policy testUTM;
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
      log {
        session-init;
        session-close;
      }
    }
  }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security utm]**.

```

feature-profile {
  web-filtering {
    type juniper-local;
  }
}

```

```

    }
  }
  utm-policy testUTM {
    web-filtering {
      http-profile junos-wf-local-default;
    }
    anti-spam {
      smtp-profile junos-as-defaults;
    }
  }
  traffic-options {
    sessions-per-client {
      over-limit log-and-permit;
    }
  }
}

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_0 {
  rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bff38-appFwRule {
    match {
      dynamic-application junos:FACEBOOK-APP;
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}

```

The hierarchy level for the following configuration sample is **[edit services user-identification identity-management]**.

```

connection {
  connect-method https;
  port 443;
  primary {
    address 10.213.50.50;
  }
}

```

```

    client-id 1234;
    client-secret "$ABC123"; ## SECRET-DATA
  }
  token-api oauth_token/oauth;
  query-api user_query/v2;
}
batch-query {
  items-per-batch 200;
  query-interval 5;
}
ip-query {
  query-delay-time 15;
}

```

Example 12: Firewall Policy that blocks access to Internet and allow access to Google Drive.

The following section provides a sample firewall policy to block access to Internet and allow access to Google Drive. The firewall policy has one enterprise-based intent and one zone-based intent.

An enterprise-based intent to block access to Internet is provided in [Table 139 on page 503](#).

Table 139: Sample Enterprise-based Intent

Rule Name	Source Endpoint	Destination Endpoint	Action
EnterpriseIntent_1	Engg (Department)	Internet	Deny

A zone-based intent to allow access to Google drive is provided in [Table 140 on page 503](#).

Table 140: Sample Zone based Intent

Rule Name	Source Endpoint	Destination Endpoint	Action
ZoneIntent_1	Engg (Zone)	untrust(zone), google-drive	Allow

The intents in [Table 139 on page 503](#) and [Table 140 on page 503](#) result in firewall rules order that is provided in [Table 141 on page 503](#).

Table 141: Sample firewall rule

Rule Name	Rule Order	Source Endpoint	Destination Endpoint	Action
ZoneIntent_1	1	Engg (Zone)	untrust(zone), google-drive	Allow
EnterpriseIntent_1	2	Engg (Department)	Internet	Deny

RELATED DOCUMENTATION

[Firewall Policy Overview | 441](#)

[Adding Firewall Policy Intents | 449](#)

Firewall Policy Schedules Overview

A schedule allows a policy to be active for a specified duration. If you want a policy to be active during a scheduled time, you must first create a schedule for that policy or link the policy to an existing schedule. When a schedule timeout expires, the associated policy is deactivated and all sessions associated with the policy are also timed out.

If a policy contains a reference to a schedule, that schedule determines when the policy is active. When a policy is active, it can be used as a possible match for traffic. A schedule lets you restrict access to, or remove a restriction from a resource, for a period of time.

A schedule uses the following guidelines:

- A schedule can have multiple policies associated with it; however, a policy cannot be associated with multiple schedules.
- A policy remains active as long as the schedule it refers to is also active.

A schedule can be active during a single time slot, as specified by a start date and time, and a stop date and time.

- A schedule can be active forever (recurrent), but only as specified by the daily schedule. The schedule on a specific day (time slot) takes priority over the daily schedule.
- A scheduler can be active during a time slot, as specified by the weekday schedule.
- A scheduler be active within two different time slots (daily or for a specified duration).

RELATED DOCUMENTATION

[About the Firewall Policy Schedules Page | 505](#)

[Firewall Policy Examples | 464](#)

[Creating Schedules | 506](#)

[Editing, Cloning, and Deleting Schedules | 508](#)

About the Firewall Policy Schedules Page

To access this page, select **Configuration > Firewall > Schedules**.

The **Firewall Policy Schedules** page enables you to create, modify, clone, and delete schedules. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a firewall policy schedule. See [“Creating Schedules” on page 506](#).
- Modify, clone, or delete a firewall policy schedule. See [“Editing, Cloning, and Deleting Schedules” on page 508](#).
- View the configured parameters of a schedule. Click the details icon that appears when you hover over the name of an image or click **More > Detailed View**.
- Show or hide columns about the firewall policy schedule. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a specific firewall policy schedule. Click the Search icon in the top right corner of the page to search for a firewall policy schedule.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

[Table 142 on page 505](#) provides guidelines on using the fields on the **Firewall Policy Schedules** page.

Table 142: Fields on the Firewall Policy Schedules Page

Field	Description
Name	Name of the schedule; maximum length is 63 characters.
Description	Description for the schedule; maximum length is 900 characters.
Start Date	The date and time from when the schedule comes into effect.
End Date	The date and time from when the schedule ends.
Second Start Date	The second date and time from when the schedule comes into effect.

Table 142: Fields on the Firewall Policy Schedules Page (continued)

Field	Description
Second End Date	The second date and time from when the schedule ends.

RELATED DOCUMENTATION

Firewall Policy Schedules Overview 504
Firewall Policy Examples 464
Creating Schedules 506
Editing, Cloning, and Deleting Schedules 508

Creating Schedules

Use the **Create Schedules** page to create schedules. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

To configure a schedule:

1. Select **Configuration > Firewall > Schedules**.
The **Firewall Policy Schedules** page appears.
2. Click the add icon (+).
The **Create Schedules** page appears.
3. Complete the configuration of the schedule according to the guidelines provided in [Table 143 on page 507](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new schedule is created. You can use this schedule to activate firewall policies for the times and dates configured in your schedules.

[Table 143 on page 507](#) provides guidelines on using the fields to create a schedule.

Table 143: Fields on the Create Schedules Page

Field	Description
General Information	
Name	Required. Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your service. You should make this description as useful as possible for all administrators.
Dates	
Date Range	<p>Select Ongoing if you want your schedules to always be active.</p> <p>Select Custom to configure two sets of start and end dates for a single schedule. For the first set, enter dates in the Start Date and End Date fields. You must enter the days in MM/DD/YYYY format.</p> <p>For the second set of the schedule, enter the start date in the Second Start Date field and enter the end date in the Second End Date field.</p>
Times	
Time Ranges	Create a schedule to be active daily or for any specific times of the day.
Daily Options	<p>Select Daily to make the schedule applicable daily.</p> <p>Select Custom to enter specific days and times. Click on a specific day to specify time options for an entire day, to exclude a specific day, or to enter time ranges for the selected day. You must enter the time in HH:MM:SS format.</p> <p>For example, if you click on Monday, you get a dialog box that allows you to specify whether you want the schedule to be active all day Monday, exclude Monday from the schedule, or have the schedule be active at specific times.</p> <p>Select Specify the same time for all days to enter a date and time that is applicable for all days.</p>

RELATED DOCUMENTATION

[Firewall Policy Schedules Overview | 504](#)
[About the Firewall Policy Schedules Page | 505](#)
[Firewall Policy Examples | 464](#)

Editing, Cloning, and Deleting Schedules

IN THIS SECTION

- [Editing Schedules | 508](#)
- [Cloning Schedules | 508](#)
- [Deleting Schedules | 509](#)

You can edit, clone, and delete schedules from the **Firewall Policy Schedules** page.

Editing Schedules

To modify the parameters configured for a schedule:

1. Select **Configuration > Firewall > Schedules**.

The **Firewall Policy Schedules** page appears.

2. Select the schedule that you want to edit, and then click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit Schedule**.

The **Edit Schedules** page appears, showing the same options as when creating a new schedule.

3. Modify the parameters according to the guidelines provided in [“Creating Schedules” on page 506](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the modified schedule appears on the **Firewall Policy Schedules** page.

Cloning Schedules

To clone a schedule:

1. Select **Configuration > Firewall Policy > Schedules**.

The **Firewall Policy Schedules** page appears.

2. Right-click on the schedule that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone Schedules** page appears with editable fields. You can modify the parameters according to the guidelines provided in [“Creating Schedules” on page 506](#).

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the cloned schedule appears under the scheduled it is cloned from, in the **Firewall Policy Schedules**.

Deleting Schedules

To delete a schedule:

1. Select **Configuration > Firewall Policy > Schedules**.

The **Firewall Policy Schedules** page appears.

2. Select the schedule you want to delete and then click the delete icon **(X)** .

An alert message appears, verifying that you want to delete the schedule.

3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected schedule is deleted.

RELATED DOCUMENTATION

Firewall Policy Schedules Overview 504
About the Firewall Policy Schedules Page 505
Creating Schedules 506
Firewall Policy Examples 464

Deploying Firewall Policies

After adding the intents to the firewall policies, you can deploy the firewall policy by clicking the **Deploy** option that is above the **End Points** panel. You can also deploy one or more policies from the **Firewall Policy** page.

To deploy firewall policies:

1. Select **Configuration > Firewall > Firewall Policy**.

The Firewall Policy page appears.

2. Select one or more policies and click **Deploy**.

The Deploy page appears.

3. In **Choose Deployment Time** options, select **Run Now** to deploy the policy immediately. Select **Schedule at a later time** and specify the date and time at which the policy should be deployed.

4. Click **Deploy**.

A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

NOTE: During deployment, CSO ensures the order of the zone-based intents and enterprise-based intents within and across the policies.

About the Default Profiles for Unified Firewall Policy Page

To access this page, select **Configuration > Firewall > Default Settings**.

Use this page to view and edit the default settings for unified firewall policies. In a unified firewall policy, dynamic application is used as a match criteria and therefore a separate application firewall is not configured on a device (CPE or next-generation firewall) to allow or block traffic to an application.

The unified firewall takes some time to detect the application in a traffic and act upon it. The default profiles help in providing security during that time.

NOTE: The unified firewall policy settings are applied on a device only when Junos OS version 18.2R1 or later is installed on the device.

The default settings comprise the following:

- A UTM profile to define antispam, antivirus, content filtering and web filtering behavior.
- An SSL proxy profile to define the action to be taken when server certificates are not authenticated.

- An IPS profile to define the actions to be taken when the traffic matches the attack objects specified in the IPS profile.
- Reject Settings to define an action when the firewall blocks traffic for a particular application:
 - Take no action
 - Provide a redirect URL to redirect the traffic to another application or URL.
 - Provide a block message to display or log a message indicating that the traffic for the particular application is blocked by the firewall policy.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the default unified firewall settings—See [Table 144 on page 511](#) describes the fields on this page.
- Modify the default profiles for the unified firewall policy—See [“Editing Default Settings for the Unified Firewall Policy” on page 512](#).

Field Descriptions

[Table 144 on page 511](#) describes the fields on the Default Profiles for the Unified Firewall Policy page.

Table 144: Default Profiles for the Unified Firewall Policy Page

Setting	Guideline
Default UTM Policy	UTM profile assigned for the unified firewall policy, which is set the default UTM policy.
Default SSL Profile	SSL proxy profile assigned for the unified firewall policy, which is set as the default SSL proxy profile.
Default IPS Profile	IPS profile assigned for the unified firewall policy, which is set as the default IPS policy on the device.
<i>Reject Settings</i>	
Reject Action	<p>The action assigned to the unified firewall policy when a firewall blocks application traffic:</p> <ul style="list-style-type: none"> • None: No message or redirection is provided. • Redirect URL: The firewall redirects the traffic to the specified URL. • Text: The firewall displays or logs the message configured for this field.

RELATED DOCUMENTATION

| [About the Firewall Policy Name Page](#) | 444

Editing Default Settings for the Unified Firewall Policy

Use the Default Profiles for Unified Firewall Policy page to configure the default profile, SSL proxy profile, IPS profile,, and reject or redirect URL or message in the unified firewall policy for a tenant. If you enable a default SSL proxy profile for the tenant, CSO sets the default SSL proxy profile for the tenant as the the default SSL profile in the unified firewall policy.

The unified firewall takes some time to detect the application in a traffic and act upon it. The default profiles help in providing security during that time. The default settings are applicable to all the unified firewall policies belonging to a tenant and pushed to all those sites where a firewall policy is deployed.

To configure default settings for the unified firewall policy:

1. Select **Configuration > Firewall > Default Settings** in Customer Portal.

The Default Profiles for Unified Firewall Policy Settings page appears.

2. Click the **Edit** button.

The fields on the page can now be modified.

3. Complete the configuration according to the guidelines provided in [Table 145 on page 513](#).

4. Do one of the following:

- Click **Cancel** to cancel the changes.
- Click **OK** to save the changes.

The settings are saved and a confirmation message is displayed.

You can deploy the changes by editing the unified firewall policy and then redeploying it.

Table 145: Default Profiles for the Unified Firewall Policy

Setting	Guideline
Default UTM Policy	<p>Select a default UTM profile (policy) from the drop-down list.</p> <p>Alternatively, click the Add UTM Profile to add a UTM profile and use it as the default UTM profile.</p> <p>The Create UTM Profiles wizard appears. For information about creating an UTM policy, see “Creating UTM Profiles” on page 525.</p>
Default SSL Profile	<p>Select a default SSL proxy profile from the drop-down list.</p> <p>Alternatively, click Add SSL Profile to add a new SSL proxy profile and use it as the default SSL proxy profile. .</p> <p>The Create SSL Proxy Profiles page appears. For information about configuring SSL proxy profiles, See “Creating SSL Forward Proxy Profiles” on page 729.</p>
Default IPS Profile	<p>Select the IPS profile that you want to associate with the unified firewall policy as the default IPS profile.</p>
<i>Reject Settings</i>	
Reject Action	<p>When the action of the firewall is set to deny a particular application traffic, provide an alternative URL to redirect such traffic or a reason for blocking the traffic and an action that a user can perform.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> • None: Do nothing when an application’s traffic is blocked by the firewall. • Redirect URL: Redirect traffic to a specified URL when the firewall blocks the traffic. If you select this option, you must specify the URL to which traffic should be redirected (in the Redirect URL field). • Text: Block traffic and display a message. If you select this option, you must enter the message (in the Block Message field) to be displayed or logged when the firewall blocks the traffic.
Redirect URL	<p>If you chose Redirect URL for Reject Action, enter the URL to which an application traffic must be redirected.</p>
Text	<p>If you choose Text for Reject Action, enter the reason for blocking the traffic and what a user can do subsequently.</p> <p>You can enter a maximum of 256 alphanumeric characters including spaces.</p>

RELATED DOCUMENTATION

[UTM Overview](#) | 519

[SSL Forward Proxy Overview](#) | 710

Importing Policies Overview

CSO supports importing policy configurations from next-generation firewall devices. You can discover existing policy configuration while onboarding next-generation firewall device (without enabling ZTP) or import policy configurations from Firewall and NAT policy pages (after ZTP).. For more information about overview and configuration of ZTP on SRX Series devices, see [Zero Touch Provisioning on SRX Series Devices](#).

- To import policy configuration after ZTP , see [“Importing Firewall Policies” on page 516](#), and [“Importing NAT Policies” on page 662](#).
- To discover existing policy configuration while onboarding next-generation firewall device (without enabling ZTP), see [“Add a Standalone Next-Generation Firewall Site” on page 153](#).

CSO uses object name as the unique identifier for an object (such as addresses, services, schedulers, SSL profiles, unified threat management (UTM), and Layer 7 applications). During policy import, all objects that are supported by CSO are imported and all objects names are compared between what is in CSO and what is on the next generation firewall device. A conflict occurs when the name of the object to be imported matches an existing object, but the value of the object does not match. The object conflict resolution (OCR) operation is triggered to resolve the object name conflicts.

- If the object name does not exist in CSO, the object is added to CSO.
- If the object name exists in CSO with the same content, the existing object in CSO is used.
- If the object name exists in CSO with different content, the object conflict resolution operation is triggered, providing users with the following conflict resolution options:
 - Rename object
 - This is the default option.
 - By default, "_1" is added to the object name, or users can specify a new unique name.
 - Deploying the policy will delete the original object and add the object with the new name.
 - There is no functional change to the firewall policy (labels only).
 - Overwrite with imported value
 - The object in CSO is replaced with the object from the import operation.
 - The change will be reflected for all other devices that use this object after the policy deployment.

- There is no functional change to the firewall policy.
- There may be possible traffic impact to all other devices that use this object the next time the other device is updated from CSO.
- Keep existing object
 - The object name in CSO is used instead of what is on the next generation firewall device.
 - Policy deployment for the imported firewall policy will show the modification.
 - There may be possible traffic impact to this firewall because the content is different in some way.

The following section provides an example for importing policies. Here we use Address as an object type and see how to resolve the object name conflicts.

The existing objects in CSO are listed in [Table 146 on page 515](#).

Table 146: Existing address in CSO

Object Name	Existing Value
Address1	198.51.100.10
Address2	198.51.100.20
Address3	198.51.100.30

The existing objects in the next generation firewall device are listed in [Table 147 on page 515](#).

Table 147: Existing address in next-generation firewall device

Object Name	Existing Value
Address1	203.0.113.10/32
Address2	203.0.113.20/32
Address3	203.0.113.30/32

During policy import, OCR is triggered and the object conflicts between next generation firewall device and CSO. The resolution that we have chosen is listed in [Table 148 on page 515](#).

Table 148: OCR while importing policies to CSO

Object Name in CSO	Object Type in CSO	Existing Value in CSO	Imported Value to CSO	Conflict Resolution	New Object Name in CSO
Address1	Address	198.51.100.10	203.0.113.10	Keep Existing Object	Address1_1

Table 148: OCR while importing policies to CSO (continued)

Object Name in CSO	Object Type in CSO	Existing Value in CSO	Imported Value to CSO	Conflict Resolution	New Object Name in CSO
Address2	Address	198.51.100.20	203.0.113.20	Overwrite with Imported value	Address2_1
Address3	Address	198.51.100.30	203.0.113.30	Rename Object	Address3_1

The object values and the result after resolving conflicts are listed in [Table 149 on page 516](#).

Table 149: After importing policies to CSO

Discovered Object Name in CSO	Discovered Value in CSO	Result
Address1	198.51.100.10	No change
Address2	203.0.113.20	Content changed
Address3	198.51.100.30	No change
Address3_1	203.0.113.30	Address3_1 created

RELATED DOCUMENTATION

Deployment Guide

Importing Firewall Policies

Use this page to manually import a firewall policy from the discovered or onboarded sites (next generation firewall sites).

To import a firewall policy:

1. Select **Configuration > Firewall > Firewall Policy**.

The Firewall Policy page appears.

2. Click **Import**.

The Import Firewall Policies page appears displaying a list of discovered devices (next generation firewall devices).

3. Select the devices from which you want to import the firewall policies and click **Next**.

The Discovered Services tab appears.

4. Select the policies that you want to import and click **Next**.

The Resolve Conflicts tab appears.

5. If there are any conflicts with the imported objects, object conflict resolution(OCR) operation is triggered. The Conflicts window displays all the conflicts between CSO and the next generation firewall device. Select an object from the Conflicts window and click on any of the below option to resolve the object conflict.

The resolution options are:

- Rename Object—Rename the imported object. By default, "_1" is added to the object name, or you can specify a new name.
- Overwrite with imported value—The object in CSO is replaced with the object from the import operation.
- Keep existing object—The object name in CSO is used instead of what is on the next generation firewall device.

6. Click **Finish**.

A summary of the discovered services is listed.

7. Review the summary and click **OK** to import the firewall policies.

The import policy job is created and the firewall policies are imported from next generation firewall device to CSO. You can view the imported policy from the Firewall Policy page.

WHAT'S NEXT

After importing the firewall policy successfully, you can edit and deploy the policy. See [Editing and Deleting Firewall Policies | 447](#), [Editing, Cloning, and Deleting Firewall Policy Intents | 455](#), and [Deploying Firewall Policies | 509](#).

RELATED DOCUMENTATION

[Importing Policies Overview | 514](#)

Managing UTM Profiles

IN THIS CHAPTER

- UTM Overview | 519
- Configuring UTM Settings | 521
- About the UTM Profiles Page | 523
- Creating UTM Profiles | 525
- Editing, Cloning, and Deleting UTM Profiles | 528
- About the Web Filtering Profiles Page | 530
- Creating Web Filtering Profiles | 532
- Editing, Cloning, and Deleting Web Filtering Profiles | 536
- About the Antivirus Profiles Page | 538
- Creating Antivirus Profiles | 540
- Editing, Cloning, and Deleting Antivirus Profiles | 543
- About the Antispam Profiles Page | 545
- Creating Antispam Profiles | 546
- Editing, Cloning, and Deleting Antispam Profiles | 548
- About the Content Filtering Profiles Page | 550
- Creating Content Filtering Profiles | 552
- Editing, Cloning, and Deleting Content Filtering Profiles | 556
- About the URL Patterns Page | 558
- Creating URL Patterns | 559
- Editing, Cloning, and Deleting URL Patterns | 560
- About the URL Categories Page | 562
- Creating URL Categories | 563
- Editing, Cloning, and Deleting URL Categories | 565

UTM Overview

IN THIS SECTION

- [UTM Licensing | 520](#)
- [UTM Components | 520](#)

Unified threat management (UTM) is a term used to describe the consolidation of several security features to protect against multiple threat types. The advantage of UTM is a streamlined installation and management of multiple security capabilities.

The following security features are provided as part of the UTM solution:

- **Antispam**—This feature examines transmitted messages to identify e-mail spam. E-mail spam consists of unwanted messages usually sent by commercial, malicious, or fraudulent entities. When the device detects an e-mail message deemed to be spam, it either drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated Spamhaus Block List (SBL). Sophos updates and maintains the IP-based SBL.
- **Full file-based antivirus**—A virus is an executable code that infects or attaches itself to other executable code to reproduce itself. Some malicious viruses erase files or lock up systems. Other viruses merely infect files and overwhelm the target host or network with bogus data. The full file-based antivirus feature provides file-based scanning on specific application layer traffic, checking for viruses against a virus signature database. The antivirus feature collects the received data packets until it has reconstructed the original application content, such as an e-mail file attachment, and then scans this content.
- **Express antivirus**—Express antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. The express antivirus feature is similar to the antivirus feature in that it scans specific application layer traffic for viruses against a virus signature database. However, unlike full antivirus, express antivirus does not reconstruct the original application content. Rather, it just sends (streams) the received data packets, as is, to the scan engine. With express antivirus, the virus scanning is executed by a hardware pattern-matching engine. This improves performance while scanning is occurring, but the level of security provided is lessened. Juniper Networks provides the scan engine.
- **Content filtering**—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.
- **Web filtering**—Web filtering enables you to manage Internet usage by preventing access to inappropriate Web content. The following types of Web filtering solutions are available:

- Integrated Web filtering—Blocks or permits Web access after the device identifies the category for a URL either from user-defined categories or from a category server (Websense provides the SurfControl Content Portal Authority (CPA) server).
- Redirect Web filtering—Intercepts HTTP requests and forwards the server URL to an external URL filtering server to determine whether to block or permit the requested Web access. Websense provides the URL filtering server.

UTM Licensing

All UTM components require licenses with the exception of content filtering, which uses the parameters defined in the content filtering profile. This is because Juniper Networks leverages third-party technology that is constantly updated to provide the most up-to-date inspection capabilities.

UTM Components

UTM components include custom objects, feature profiles, and UTM profiles that can be configured on SRX Series devices. From a high level, feature profiles specify how a feature is configured and then applied to UTM profiles, which in turn is applied to firewall policies, as shown in [Figure 20 on page 520](#).

Figure 20: UTM Components



UTM profiles do not have their own seven-tuple rulebase; in a sense they inherit the rules from the firewall rule. The strength of the UTM feature comes from URL filtering, where you can have a separate configuration for different users or user groups.

- Custom objects—Although SRX Series devices support predefined feature profiles that can handle most typical use cases, there are some cases where you might need to define your own objects, specifically for URL filtering, antivirus filtering, and content filtering.
- Feature profiles—Feature profiles specify how components of each profile should function. You can configure multiple feature profiles that can be applied through different UTM profiles to firewall rules.
- UTM profiles—UTM profiles function as a logical container for individual feature profiles. UTM profiles are then applied to specific traffic flows based on the classification of rules in the firewall policy, thereby enabling you to define separate UTM profiles per firewall rule to differentiate the enforcement per

firewall rule. Essentially, the firewall rulebase acts as the match criteria, and the UTM profile is the action to be applied.

- Firewall policy—You can predefine feature profiles for the UTM profile that are then applied to the firewall rules. This gives you the advantage of using the predefined UTM profile for that one UTM technology (for example, antivirus or URL filtering), not both.

RELATED DOCUMENTATION

Configuring UTM Settings 521
About the UTM Profiles Page 523
Creating UTM Profiles 525

Configuring UTM Settings

Use the Edit UTM Settings page to configure unified threat management (UTM) antispam, antivirus, and Web filtering settings for a tenant.

These settings are applicable to all the sites belonging to a tenant. The settings are pushed to all those sites where a firewall policy intent with UTM enabled is applicable.

To configure UTM settings:

1. Select **Configuration > Unified Threat Mgmt > UTM Settings** in Customer Portal.
The Edit UTM Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 150 on page 521](#).
3. Do one of the following:
 - Click **Reset** to reset the settings to the previously saved configured.
 - Click **OK** to save the settings.

The settings are saved and a confirmation message is displayed.

Table 150: UTM Settings

Setting	Guideline
Antispam Settings	

Table 150: UTM Settings (*continued*)

Setting	Guideline
Address Whitelist	<p>Select the URL pattern to be used as the antispam allowlist.</p> <p>Alternatively, click Create a New Pattern to create a new URL pattern to use as a allowlist.</p> <p>The Create URL Patterns page appears. For more information, see “Creating URL Patterns” on page 559 for an explanation of the fields on this page.</p>
Address Blacklist	<p>Select the URL pattern to be used as the antispam blocklist.</p> <p>Alternatively, click Create a New Pattern to create a new URL pattern to use as a blocklist.</p>
Antivirus Settings	
MIME Whitelist	Enter one or more MIME types (separated by commas) to exclude from antivirus scanning.
Exception MIME Whitelist	Enter one or more MIME types (separated by commas) that are to be excluded from the list of MIME types specified as part of the MIME allowlist. This list is a subset of the MIME types that you specified in the MIME allowlist. For example, if you specify video/ in the allowlist and video/x-shockwave-flash in the exception allowlist, all objects of MIME type video/ except MIME type video/x-shockwave-flash are excluded from antivirus scanning.
URL Whitelist	Select the list of URLs the antivirus settings can allow.
Web Filtering Settings	
URL Whitelist	Select the list of URLs the Web filtering settings can allow; these URLs are excluded from Web filtering.
URL Blacklist	Select the list of URLs the Web filtering settings can block; these URLs are blocked from Web access.

RELATED DOCUMENTATION

| [About the UTM Profiles Page](#) | 523

About the UTM Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

Use this page to view and manage unified threat management (UTM) profiles. UTM profiles enable you to consolidate several security features into one system to protect against multiple threat types.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a UTM profile—See [“Creating UTM Profiles” on page 525](#).
- Edit, clone, or delete a UTM profile—See [“Editing, Cloning, and Deleting UTM Profiles” on page 528](#).
- Clear the selected UTM profiles—Click **Clear All Selections** to clear any UTM profiles that you might have selected.
- View the details of a UTM profile—Select the UTM profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The UTM Profile Details page appears. [Table 152 on page 524](#) describes the fields on this page.
- Search for UTM profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 151 on page 523](#) describes the fields on the UTM Profiles page.

Table 151: UTM Profiles Page Fields

Field	Description
Name	Name of the UTM profile.
Antispam	Information about the antispam profile associated with the UTM profile.
Antivirus	Information about the antivirus profiles associated with the UTM profile.
Content Filtering	Information about the content filtering profiles associated with the UTM profile.
Web Filtering	Information about the Web filtering profile associated with the UTM profile.
Description	Description of the UTM profile.

Table 152: UTM Profile Details Page Fields

Field	Description
General Information	
Name	Name of the UTM profile.
Description	Description of the UTM profile.
Traffic Options	
Action When Connection Limit Is Reached	Action to be taken when the configured connection limit per client is reached.
Web Filtering Profile	
HTTP	Web filtering profile to be used for HTTP traffic.
Antivirus Profile	
HTTP	Antivirus profile to be used for HTTP traffic.
FTP Upload	Antivirus profile to be used for FTP upload traffic.
FTP Download	Antivirus profile to be used for FTP download traffic.
IMAP	Antivirus profile to be used for IMAP traffic.
SMTP	Antivirus profile to be used for SMTP traffic.
POP3	Antivirus profile to be used for POP3 traffic.
Antispam Profile	
SMTP	Antispam profile to be used for SMTP traffic.

RELATED DOCUMENTATION

[Creating UTM Profiles](#) | 525

Creating UTM Profiles

Use the Create UTM Profiles page to configure UTM profiles. Unified threat management (UTM) consolidates several security features to protect against multiple threat types. The Create UTM Profiles wizard provides step-by-step procedures to create a UTM profile. You can configure antispam, antivirus, Web filtering, and content filtering profiles by launching the respective wizards from the wizard.

To create a UTM profile:

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears.

2. Click the add icon (+) to create a new UTM profile.

The Create UTM Profiles wizard appears, displaying brief instructions about creating a UTM profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 153 on page 525](#).

NOTE: Fields marked with * are mandatory.

5. Click **Finish**.

A UTM profile is created. You are returned to the UTM Profiles page where a confirmation message is displayed. After you create a UTM profile, you can assign it to a firewall policy intent on the Firewall Policy page.

Table 153: UTM Profile Settings

Setting	Guideline
General	
Name	Enter a unique name for the UTM profile. The maximum length is 29 characters.
Description	Enter a description for the UTM profile. The maximum length is 255 characters.
Traffic Options	
<p>NOTE: In an attempt to consume all available resources, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose traffic options.</p>	

Table 153: UTM Profile Settings (*continued*)

Setting	Guideline
Connection Limit per Client	Specify the connection limit per client for client connections on the device. The default is 2000 and a value of 0 means that there is no connection limit.
Action when connection limit is reached	Specify the action that must be taken when the connection limit is reached. The available actions are No action (default), Log and permit, and Block. Click Next to continue.
Web Filtering	
HTTP	Select the Web filtering profile to be applied for HTTP traffic. Alternatively, click Create Another Profile to create a Web filtering profile. The Create Web Filtering Profiles wizard appears. See “Creating Web Filtering Profiles” on page 532 for an explanation of the fields on this wizard. Click Back to go the preceding step or click Next to go to the next step.
Antivirus	
Apply to all protocols	Select this check box to apply a single antivirus profile to all traffic protocols. and then specify the profile in the Default Profile field. Clear the check box if you want to apply traffic-specific profiles.
Default Profile	Select the antivirus profile to be applied to all traffic protocols. Click Back to go the preceding step or click Next to go to the next step.
NOTE: Click Create Another Profile to create an antivirus profile that you can then assign. The Create Antivirus Profiles wizard appears. See “Creating Antivirus Profiles” on page 540 for an explanation of the fields on this wizard.	
HTTP	Select the antivirus profile to be applied to HTTP traffic.
FTP Upload	Select the antivirus profile to be applied to FTP upload traffic.
FTP Download	Select the antivirus profile to be applied to FTP download traffic.
IMAP	Select the antivirus profile to be applied to IMAP traffic.
SMTP	Select the antivirus profile to be applied to SMTP traffic.

Table 153: UTM Profile Settings (*continued*)

Setting	Guideline
POP3	<p>Select the antivirus profile to be applied to POP3 traffic.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Antispam	
SMTP	<p>Select the antispam profile to be applied for SMTP traffic.</p> <p>Alternatively, click Create Another Profile to create an antispam profile. The Create Antispam Profiles wizard appears. See “Creating Antispam Profiles” on page 546 for an explanation of the fields on this wizard.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Content Filtering	
Apply to all protocols	<p>Select this check box to apply a single content filtering profile to all traffic protocols, and then specify the profile in the Default Profile field.</p> <p>Clear the check box if you want to apply traffic-specific profiles.</p>
Default Profile	<p>Select the content filtering profile to be applied to all traffic protocols.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
<p>NOTE: Click Create Another Profile to create a content filtering profile that you can then assign. The Create Content Filtering Profiles wizard appears. See “Creating Content Filtering Profiles” on page 552 for an explanation of the fields on this wizard.</p>	
HTTP	Select the content filtering profile to be applied to HTTP traffic.
FTP Upload	Select the content filtering profile to be applied to FTP upload traffic.
FTP Download	Select the content filtering profile to be applied to FTP download traffic.
IMAP	Select the content filtering profile to be applied to IMAP traffic.
SMTP	Select the content filtering profile to be applied to SMTP traffic.
POP3	<p>Select the content filtering profile to be applied to POP3 traffic.</p> <p>Click Back to go the preceding step.</p>

RELATED DOCUMENTATION

[About the UTM Profiles Page | 523](#)

[Configuring UTM Settings | 521](#)

Editing, Cloning, and Deleting UTM Profiles

IN THIS SECTION

- [Editing UTM Profiles | 528](#)
- [Cloning UTM Profiles | 529](#)
- [Deleting UTM Profiles | 529](#)

You can edit, clone, and delete UTM profiles from the UTM Profiles page. This topic has the following sections:

Editing UTM Profiles

To modify the parameters configured for a UTM profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears, displaying the existing UTM profiles.

2. Select the UTM profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.

The Edit UTM Profiles page appears, displaying the same fields that are presented when you create a UTM profile.

3. Modify the UTM profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the UTM Profiles page. A confirmation message appears indicating the status of the edit operation.

Cloning UTM Profiles

Cloning enables you to easily create a new UTM profile based on an existing one.

To clone a UTM profile:

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears, displaying the existing UTM profiles.

2. Select the UTM profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone UTM Profiles page appears, displaying the same fields that are presented when you create a UTM profile.

3. Modify the UTM profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the UTM Profiles page. A confirmation message appears, indicating the status of the clone operation.

Deleting UTM Profiles

NOTE: Before deleting a UTM profile, ensure that the profile is not used in a firewall policy intent. If you try to delete a profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more UTM profiles:

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears, displaying the existing UTM profiles.

2. Select one or more UTM profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete Profile**.

An alert message appears, asking you to confirm the delete operation.

- Click **Yes** to delete the selected UTM profiles.
A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

Creating UTM Profiles 525
About the UTM Profiles Page 523

About the Web Filtering Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.

Use the Web Filtering Profiles page to view and manage Web filtering profiles. Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. [Table 154 on page 530](#) lists the Web filtering solutions that are supported and the license requirements.

Table 154: Web Filtering Solutions Supported

Type	Description	License Requirement
Integrated Web Filtering	Blocks or permits Web access after the device identifies the category for a URL, either from user-defined categories or from a category server (SurfControl Content Portal Authority provided by Websense).	A separately licensed subscription service
Redirect Web Filtering	Intercepts HTTP requests and forwards the server URL to an external URL filtering server to determine whether to block or permit the requested Web access. Websense provides the URL filtering server.	Does not require a license.
Juniper Local Web Filtering	Intercepts every HTTP request in a TCP connection. In this case, the decision making is done on the device after it looks up a URL to determine whether it is in the allowlist or blocklist based on its user-defined category.	Does not require a license or a remote category server

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a Web filtering profile—See [“Creating Web Filtering Profiles” on page 532](#).
- Edit, clone, or delete a Web filtering profile—See [“Editing, Cloning, and Deleting Web Filtering Profiles” on page 536](#).
- Clear the selected Web filtering profiles—Click **Clear All Selections** to clear any Web filtering profiles that you might have selected.
- View the details of a Web filtering profile—Select the Web filtering profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Web Filtering Profile Details page appears. [Table 156 on page 531](#) describes the fields on this page.
- Search for Web filtering profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 155 on page 531](#) describes the fields on the Web Filtering Profiles page.

Table 155: Web Filtering Profiles Page Fields

Field	Description
Name	Name of the Web filtering profile.
Profile Type	Type of engine used for the profile: Juniper-enhanced or Websense redirect.
Default Action	Default action taken when the specified connection limit per client is reached.
Timeout	
Description	Description of the Web filtering profile.

Table 156: Web Filtering Profile Details Page Fields

Field	Description
General Information	
Name	Name of the Web filtering profile.
Description	Description of the Web filtering profile.
Engine Type	Type of engine used for the profile: Juniper-enhanced or Websense redirect.
Default Action	Default action taken when the specified connection limit per client is reached.

Table 156: Web Filtering Profile Details Page Fields (*continued*)

Field	Description
Fallback Options	
Default Action	Action taken for URL categories with no assigned action and for uncategorized URLs. This action is taken only if no reputation action is assigned.
Global Reputation Actions	Actions taken for the following site reputations: <ul style="list-style-type: none"> • Very Safe • Moderately Safe • Fairly Safe • Suspicious • Harmful
URL Categories	URL categories associated with the Web filtering profile.

RELATED DOCUMENTATION

[Creating Web Filtering Profiles | 532](#)
[Editing, Cloning, and Deleting Web Filtering Profiles | 536](#)

Creating Web Filtering Profiles

Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP.

To create a Web filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.

The Web Filtering Profiles page appears.

2. Click the add icon (+) to create a new Web filtering profile.

The Create Web Filtering Profiles wizard appears, displaying brief instructions about creating a Web filtering profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 157 on page 533](#).

NOTE: Fields marked with * are mandatory.

5. Click **Finish**.

A Web filtering profile is created, which you can associate with a UTM profile. You are returned to the Web Filtering Profiles page where a confirmation message is displayed.

Table 157: Creating Web Filtering Profiles Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the Web filtering profile. The maximum length is 29 characters.
Description	Enter a description for the Web filtering profile. The maximum length is 255 characters.
Timeout	Enter a timeout (in seconds) to wait for a response from the Websense server. The default is 15 seconds and the maximum is 1000 seconds.
Engine Type	Select an engine type for Web filtering: <ul style="list-style-type: none"> • (Default) Juniper Enhanced—UTM-enhanced Web filtering. • Websense Redirect—Redirect Web filtering profile.
Safe Search	Select the check box (default) to ensure that embedded objects, such as images on the URLs received from the search engines, are safe and that undesirable content is not returned to the client. Clear the check box to disable safe search redirects. NOTE: This option is available only for the Juniper Enhanced engine type. Safe search redirect supports only HTTP and you cannot extract the URL for HTTPS. Therefore, it is not possible to generate a redirect response for HTTPS search URLs.
Custom Block Message/URL	Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. The maximum length is 512 characters. NOTE: If a message begins with http: or https:, the message is considered a block message URL. Messages that begin with values other than http: or https: are considered custom block messages. Click Back to go the preceding step or click Next to go to the next step.

Table 157: Creating Web Filtering Profiles Settings (*continued*)

Setting	Guideline
Custom Quarantine Message	<p>Define a custom message to allow or deny access to a blocked site based on a user's response to the message. The maximum length is 512 characters.</p> <p>The quarantine message contains the following information:</p> <ul style="list-style-type: none"> • URL name • Quarantine name • Category (if available) • Site reputation (if available) <p>For example, if you set the action for <code>Enhanced_Search_Engines_and_Portals</code> to quarantine, and you try to access <code>www.search.yahoo.com</code>, the quarantine message is as follows: ***The requested webpage is blocked by your organization's access policy***.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Account	Specify the user account associated with the Websense Web filtering profile.
Server	Specify the hostname or IP address for the Websense server.
Port	<p>Specify the port number to use to communicate with the Websense server. The default port value is 15968.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Sockets	Enter the number of sockets used for communication between the client and the server. The default value is 8.
URL Categories	
Deny Action List	<p>Click the Add URL Categories button to specify a list of URL categories that should be denied access.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 158 on page 536.</p> <p>The list of URL categories selected is displayed in a text box.</p>
Log & Permit Action List	<p>Specify a list of URL categories that are logged and then permitted.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 158 on page 536.</p> <p>The list of URL categories selected is displayed in a text box.</p>

Table 157: Creating Web Filtering Profiles Settings (*continued*)

Setting	Guideline
Permit Action List	<p>Specify a list of URL categories that should be permitted access.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 158 on page 536</p> <p>The list of URL categories selected is displayed in a text box.</p>
Quarantine Action List	<p>Specify a list of URL categories that should be quarantined.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 158 on page 536.</p> <p>The list of URL categories selected is displayed in a text box.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Fallback Options	
Global Reputation Actions	<p>Select this check box (default) if you want to apply global reputation actions.</p> <p>Enhanced Web filtering intercepts HTTP and HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the predefined categories and also provides site reputation information for the URL to the device. The device determines if it can permit or block the request based on the information provided by the TSC.</p> <p>The URLs can be processed using their reputation score if there is no category available. Select the action that you want to take for the uncategorized URLs based on their reputation score:</p> <ul style="list-style-type: none"> ● Very Safe—Permit, log and permit, block, or quarantine a request if a site reputation of 90 through 100 is returned. By default, Permit is selected. ● Moderately Safe—Permit, log and permit, block, or quarantine a request if a site reputation of 80 through 89 is returned. By default, Log and Permit is selected. ● Fairly Safe—Permit, log and permit, block or quarantine a request if a site-reputation of 70 through 79 is returned. By default, Log and Permit is selected. ● Suspicious—Permit, log and permit, block, or quarantine a request if a site reputation of 60 through 69 is returned. By default, Quarantine is selected. ● Harmful—Permit, log and permit, block, or quarantine a request if a site reputation of zero through 59 is returned. By default, Block is selected.
Default Action	<p>Choose the actions to be taken for URL categories with no assigned action and for uncategorized URLs. This is used only if no reputation action is assigned.</p>

Table 157: Creating Web Filtering Profiles Settings (*continued*)

Setting	Guideline
Fallback Action	<p>Select the fallback action, which is used when:</p> <ul style="list-style-type: none"> • The ThreatSeeker Websense Cloud servers are unreachable. • A timeout occurs for requests to ThreatSeeker Cloud. • There are too many requests to be handled by the device.

Table 158: Select URL Categories Settings

Setting	Guideline
Show	<p>Choose which URL categories should be displayed for selection: All categories, Custom URL categories, or Websense URL categories.</p> <p>The Available column of the URL Categories field displays URL categories based on your selection.</p>
URL Categories	<p>Select one or more URL categories in the Available column and click the forward arrow to confirm your selection. The selected URL categories are displayed in the Selected column.</p> <p>Alternatively, click Create New URL Category to create a URL category and assign it to the URL category. The Create URL Categories page appears; for more information, see “Creating URL Categories” on page 563.</p> <p>Click OK to confirm your selection. You are returned to the Create Web Filtering Profiles page.</p>

RELATED DOCUMENTATION

| [Creating UTM Profiles | 525](#)

Editing, Cloning, and Deleting Web Filtering Profiles

IN THIS SECTION

- [Editing Web Filtering Profiles | 537](#)
- [Cloning Web Filtering Profiles | 537](#)
- [Deleting Web Filtering Profiles | 538](#)

You can edit, clone, and delete Web filtering profiles from the Web Filtering Profiles page. This topic has the following sections:

Editing Web Filtering Profiles

To modify the parameters configured for a Web filtering profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.
The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.
2. Select the Web filtering profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.
The Edit Web Filtering Profiles page appears, displaying the same fields that are presented when you create a Web filtering profile.
3. Modify the Web filtering profile fields as needed.
4. Click **OK** to save your changes.
You are taken to the Web Filtering Profiles page. A confirmation message appears, indicating the status of the edit operation.

Cloning Web Filtering Profiles

Cloning enables you to easily create a new Web filtering profile based on an existing one.

To clone a Web filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.
The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.
2. Select the Web filtering profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.
The Clone Web Filtering Profiles page appears, displaying the same fields that are presented when you create a Web filtering profile.

3. Modify the Web filtering profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Web Filtering Profiles page. A confirmation message appears, indicating the status of the clone operation.

Deleting Web Filtering Profiles

Before deleting a Web filtering profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete a Web filtering profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more Web filtering profiles:

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.

The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.

2. Select one or more Web filtering profiles that you want to delete and click the delete icon (X).
Alternatively, right-click a profile and select **Delete Profile**.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected Web filtering profiles.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

[Creating Web Filtering Profiles | 532](#)

[About the Web Filtering Profiles Page | 530](#)

About the Antivirus Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

Use the Antivirus Profiles page to view and manage antivirus profiles. Antivirus profiles enable you to inspect files transmitted over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) to determine whether the files exchanged are known malicious files, similar to how desktop antivirus software scans files for the same purpose.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an antivirus profile—See [“Creating Antivirus Profiles” on page 540](#).
- Edit, clone, or delete an antivirus profile—See [“Editing, Cloning, and Deleting Antivirus Profiles” on page 543](#).
- Clear the selected antivirus profiles—Click **Clear All Selections** to clear any antivirus profiles that you might have selected.
- View the details of an antivirus profile—Select the antivirus profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Antivirus Profile Details page appears. [Table 160 on page 539](#) describes the fields on this page.
- Search for antivirus profiles by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 159 on page 539](#) describes the fields on the Antivirus Profiles page.

Table 159: Antivirus Profiles Page Fields

Field	Description
Name	Name of the antivirus profile.
Profile Type	Type of engine used for the profile.
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Trickling Timeout	Number of seconds to wait for a response from the server.
Description	Description of the antivirus profile.

Table 160: Antivirus Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the antivirus profile.
Description	Description of the antivirus profile.

Table 160: Antivirus Profiles Details Page Fields (*continued*)

Field	Description
Engine Type	Type of engine used for the profile.
Scan Options	
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Fallback Options	
Default Action	Displays the default fallback action taken when the antivirus system encounters errors.
Content Size	Displays the actions taken if the content size exceeds a set limit.
Engine Error	Displays the action taken when an engine error occurs.

RELATED DOCUMENTATION

| [Creating UTM Profiles](#) | 525

Creating Antivirus Profiles

Use the Create Antivirus Profiles page to configure antivirus profiles. The antivirus profile defines the content to scan for any malware and the action to be taken when malware is detected. After you create a profile, you can assign it to UTM profiles.

To create an antivirus profile:

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears.

2. Click the add icon (+) to create a new antivirus profile.

The Create Antivirus Profiles wizard appears, displaying brief instructions about creating an antivirus profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 161 on page 541](#).

NOTE: Fields marked with * are mandatory.

5. Click **Finish**.

A summary page is displayed. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.

6. Click **OK** to save the settings and create the profile.

A message indicating the status of the create operation is displayed.

7. Click **Close**.

You are returned to the Antivirus Profiles page.

Table 161: Antivirus Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antivirus profile. The maximum length is 29 characters.
Description	Enter a description for the antivirus profile. The maximum length is 255 characters.
Engine Type	Displays the engine type used for scanning. Currently, Sophos is the only antivirus engine supported. Sophos antivirus is an in-the-cloud antivirus solution. The virus and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers, thus there is no need to download and maintain large pattern databases on the Juniper Networks device.
Fallback Options	

Table 161: Antivirus Profile Settings (*continued*)

Setting	Guideline
	<p>Fallback options are used when the antivirus system experiences errors and must fall back to one of the previously configured actions to either deny (block) or permit the object.</p> <p>Specify the fallback options to use when there is a failure, or select the default action if no specific options are to be configured:</p> <ul style="list-style-type: none"> • Content Size—Select an option to specify whether the content should be blocked (default) or logged and permitted if the content size the previously defined limit. • Content Size Limit—Enter the content size limit in kilobytes (KB) based on which action is taken. The range is 20 through 40,000 KB. The content size limit check occurs before the scan request is sent. The content size refers to accumulated TCP payload size. • Engine Error—Select the action to take (Block [default] or Log and Permit) when an engine error occurs. The term <i>engine error</i> refers all engine errors, including engine not ready, timeout, too many requests, password protected, corrupt file, decompress layer, and out of resources. • Default Action—Select the default action (Block [default] or Log and Permit) to take when an error occurs.
Notification Options	
	<p>Use the notification options to configure a method of notifying the user when a fallback occurs or a virus is detected:</p> <ul style="list-style-type: none"> • Fallback Deny—Select this option to notify mail senders that their messages were blocked. • Fallback Non-Deny—Select this option to warn mail recipients that they received unblocked messages despite problems. • Virus Detected—Select this option to notify mail recipients that their messages were blocked.

RELATED DOCUMENTATION

Creating UTM Profiles | 525

Editing, Cloning, and Deleting Antivirus Profiles

IN THIS SECTION

- [Editing Antivirus Profiles | 543](#)
- [Cloning Antivirus Profiles | 543](#)
- [Deleting Antivirus Profiles | 544](#)

You can edit, clone, and delete antivirus profiles from the Antivirus Profiles page. This topic has the following sections:

Editing Antivirus Profiles

To modify the parameters configured for an antivirus profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select the antivirus profile that you want to edit and then select the edit icon (pencil). Alternatively, right-click a profile and select **Edit Antivirus Profile**.

The Edit Antivirus Profiles page appears, displaying the same fields that are presented when you create an antivirus profile.

3. Modify the antivirus profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Antivirus Profiles page. A confirmation message appears, indicating the status of the edit operation.

Cloning Antivirus Profiles

Cloning enables you to easily create a new antivirus profile based on an existing one.

To clone an antivirus profile:

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select the antivirus profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Antivirus Profiles page appears, displaying the same fields that are presented when you create an antivirus profile.

3. Modify the antivirus profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Antivirus Profiles page. A confirmation message appears, indicating the status of the clone operation.

Deleting Antivirus Profiles

Before deleting an antivirus profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete an antivirus profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more antivirus profiles:

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select one or more antivirus profiles that you want to delete and then select the delete icon (X). Alternatively, right-click a profile and select **Delete Antivirus Profiles**.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected antivirus profiles.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

[Creating Antivirus Profiles | 540](#)

[About the Antivirus Profiles Page | 538](#)

About the Antispam Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

Use the Antispam Profiles page to view and manage antispam profiles. An antispam profile is used to examine transmitted e-mail messages to identify e-mail spam by using a constantly updated spam block list.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an antispam profile—See [“Creating Antispam Profiles” on page 546](#).
- Edit, clone, or delete an antispam profile—See [“Editing, Cloning, and Deleting Antispam Profiles” on page 548](#).
- Clear the selected antispam profiles—Click **Clear All Selections** to clear any antispam profiles that you might have selected.
- View the details of an antispam profile—Select the antispam profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Antispam Profile Details page appears. [Table 163 on page 546](#) describes the fields on this page.
- Search for antispam profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 162 on page 545](#) describes the fields on the Antispam Profiles page.

Table 162: Antispam Profiles Page Fields

Field	Description
Name	Name of the antispam profile.
Blacklist	Indicates whether server-based spam filtering or local spam filtering is used.
Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.
Description	Description of the antispam profile.

Table 163: Antispam Profile Details Page Fields

Field	Description
Name	Name of the antispam profile.
Description	Description of the antispam profile.
Sophos Blacklist	Indicates whether Sophos Blacklist is enabled (server-based filtering) or disabled (local filtering).
Default Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.

RELATED DOCUMENTATION

[Creating UTM Profiles](#) | 525

Creating Antispam Profiles

Use the Create Antispam Profiles page to configure antispam profiles.

E-mail spam consists of unwanted e-mail messages usually sent by commercial, malicious, or fraudulent entities. When the device detects an e-mail message deemed to be spam, it either blocks the message or tags the message header or subject field with a preprogrammed string. Antispam filtering allows you to use a third-party server-based spam block list (SBL) and to optionally create your own local allowlists (benign) and blocklists (malicious) for filtering against e-mail messages.

NOTE: Sophos updates and maintains the IP-based SBL. Antispam is a separately licensed subscription service.

After you create an antispam profile, you can assign it to UTM profiles.

To create an antispam profile:

1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears.

2. Click the add icon (+) to create a new antispam profile.

The Create Antispam Profiles wizard appears, displaying brief instructions about creating an antispam profile.

3. Complete the configuration according to the guidelines provided in [Table 164 on page 547](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** save the settings and create the profile.

A message indicating the status of the create operation is displayed. You are returned to the Antispam Profiles page.

Table 164: Antispam Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antispam profile. The maximum length is 29 characters.
Description	Enter a description for the antispam profile. The maximum length is 255 characters.
Sophos Blacklist	<p>Select this check box (the default) to use server-based spam filtering. If you clear the check box, local spam filtering is used.</p> <p>Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. Domain Name Service (DNS) is required to access the SBL server. The firewall performs SBL lookups through the DNS protocol.</p> <p>NOTE: Server-based spam filtering supports only IP-based spam block list blocklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service.</p>
Action	

Table 164: Antispam Profile Settings (continued)

Setting	Guideline
Default Action	<p>Select the action to be taken when spam is detected:</p> <ul style="list-style-type: none"> • Tag Email Subject Line • Tag SMTP Header • Block Email • None
Custom Tag	<p>Enter a custom string for identifying a message as spam. The maximum length is 512 characters and the default is ***SPAM***.</p>

RELATED DOCUMENTATION

| [Creating UTM Profiles | 525](#)

Editing, Cloning, and Deleting Antispam Profiles

IN THIS SECTION

- [Editing Antispam Profiles | 549](#)
- [Cloning Antispam Profiles | 549](#)
- [Deleting Antispam Profiles | 550](#)

You can edit, clone, and delete antispam profiles from the Antispam Profiles page. This topic has the following sections:

Editing Antispam Profiles

To modify the parameters configured for an antispam profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears, displaying the existing antispam profiles.

2. Select the antispam profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Antispam Profile**.

The Edit Antispam Profiles page appears, displaying the same fields that are presented when you create an antispam profile.

3. Modify the antispam profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Antispam Profiles page. A confirmation message appears, indicating the status of the edit operation.

Cloning Antispam Profiles

Cloning enables you to easily create a new antispam profile based on an existing one.

To clone an antispam profile:

1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears displaying the existing antispam profiles.

2. Select the antispam profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Antispam Profiles page appears, displaying the same fields that are presented when you create an antispam profile.

3. Modify the antispam profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Antispam Profiles page. A confirmation message appears, indicating the status of the clone operation.

Deleting Antispam Profiles

Before deleting an antispam profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete an antispam profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more antispam profiles:

1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears, displaying the existing antispam profiles.

2. Select one or more antispam profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete Antispam Profiles**.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected antispam profiles.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

| [About the Antispam Profiles Page](#) | 545

About the Content Filtering Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

Use the Content Filtering Profiles page to view and manage content filtering profiles. Content filtering profiles enable you to block or permit certain types of traffic over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) based on the MIME type, file extension, protocol command, and embedded object type.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a content filtering profile—See [“Creating Content Filtering Profiles” on page 552](#).
- Edit, clone, or delete a content filtering profile—See [“Editing, Cloning, and Deleting Content Filtering Profiles” on page 556](#).
- Clear the selected content filtering profiles—Click **Clear All Selections** to clear any content filtering profiles that you might have selected.
- View the details of a content filtering profile—Select the content filtering profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Content Filtering Profile Details page appears. [Table 166 on page 551](#) describes the fields on this page.
- Search for content filtering profiles by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 165 on page 551](#) describes the fields on the Content Filtering Profiles page.

Table 165: Content Filtering Profiles Page Fields

Field	Description
Name	Name of the content filtering profile.
Permit Command List	List of protocol commands permitted by the content filtering profile.
Block Command List	List of protocol commands blocked by the content filtering profile.
Notification Type	Type of notification that is sent when content is blocked.
Description	Description of the content filtering profile.

Table 166: Content Filtering Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the content filtering profile.
Description	Description of the content filtering profile.
General Information	
Notify Mail Sender	Specifies whether the option to notify the e-mail sender is enabled or disabled.

Table 166: Content Filtering Profiles Details Page Fields (*continued*)

Field	Description
Notification Type	Type of notification that is sent when content is blocked.
Custom Notification Message	Custom notification message that is sent when content is blocked.
Protocol Commands	
Command Block List	List of protocol commands permitted by the content filtering profile.
Command Permit List	List of protocol commands blocked by the content filtering profile.
Content Types	
Block Content Types	List of harmful content types to be blocked.
File Extensions	
Extension Block List	File extensions to be blocked.
MIME	
MIME Block List	List of MIME types to be blocked.
MIME Permit List	List of MIME types to be permitted.

RELATED DOCUMENTATION

| [Creating UTM Profiles](#) | 525

Creating Content Filtering Profiles

Use the Create Content Filtering Profiles page to configure content filtering profiles. Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the device by checking traffic against configured filter lists. [Table 167 on page 553](#) displays the types of content filters that you can configure as part of a content filtering profile.

NOTE: The content filtering profile evaluates traffic before all other UTM profiles. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.

Table 167: Supported Content Filter Types

Type	Description
MIME pattern filter	<p>MIME patterns are used to identify the type of traffic in HTTP and MAIL protocols. There are two lists of MIME patterns that are used by the content filter to determine the action to be taken. The block MIME list contains a list of MIME type traffic that is to be blocked. The MIME exception list contains MIME patterns that are not to be blocked by the content filter and are generally subsets of items on the block list.</p> <p>NOTE: The exception list has a higher priority than the block list.</p>
Block Extension List	<p>Because the name of a file is available during the transfers, using file extensions is a highly practical way to block or allow file transfers. All protocols support the use of the block extension list.</p>
Protocol Command Block and Permit Lists	<p>Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level. The block or permit command lists are intended to be used in combination, with the permit list acting as an exception list to the block list.</p> <p>NOTE: If a protocol command appears on both the permit list and the block list, the command is permitted.</p>

To create a content filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears.

2. Click the add icon (+) to create a new content filtering profile.

The Create Content Filtering Profiles wizard appears, displaying brief instructions about creating a content filtering profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 168 on page 554](#).

NOTE: Fields marked with * are mandatory.

5. Click **Finish**.

A summary page is displayed. Review the settings and if you need to make any modifications click the **Edit** link or the **Back** button.

6. Click **OK** save the settings and create the profile.

A message indicating the status of the create operation is displayed.

7. Click **Close**.

You are returned to the Content Filtering Profiles page.

Table 168: Content Filtering Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the content filtering profile. The maximum length is 29 characters.
Description	Enter a description for the content filtering profile. The maximum length is 255 characters.
Notification Options	
Notify Mail Sender	Select this check box if you want to notify the sender when a failure occurs or a virus is detected. This check box is cleared by default.
Notification Type	Select the type of notification (Protocol or Message) from the drop-down list.
Custom Notification Message	Enter a custom notification message. The maximum length is 512 characters.
Protocol Commands	
Command Block List	<p>Enter the protocol commands to be blocked for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.</p> <p>Protocol commands allow you to control traffic at the protocol-command level.</p>

Table 168: Content Filtering Profile Settings (*continued*)

Setting	Guideline
Command Permit List	Enter specific commands to be permitted for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.
Content Types	
Block Content Type	<p>Use the content filter to block other types of harmful files that the MIME type or the file extension cannot control. Select from the following types of content blocking (supported only for HTTP):</p> <ul style="list-style-type: none"> • Active X • Windows executables (.exe) • HTTP cookie • Java applet • ZIP files
File Extensions	
Extension Block List	<p>Use a file extension list to define a set of file extensions to block over HTTP, FTP, SMTP, IMAP, and POP3.</p> <p>Enter file extensions to block separated by commas. For example, exe, pdf, js, and so on.</p>
MIME Types	
MIME Block List	Enter the MIME types you want to block over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.
MIME Permit List	Enter the MIME types you want to permit over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.

RELATED DOCUMENTATION

[Creating UTM Profiles](#) | 525

Editing, Cloning, and Deleting Content Filtering Profiles

IN THIS SECTION

- [Editing Content Filtering Profiles | 556](#)
- [Cloning Content Filtering Profiles | 556](#)
- [Deleting Content Filtering Profiles | 557](#)

You can edit, clone, and delete content filtering profiles from the Content Filtering Profiles page. This topic has the following sections:

Editing Content Filtering Profiles

To modify the parameters configured for a content filtering profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select the content filtering profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.

The Edit Content Filtering Profiles page appears, displaying the same fields that are presented when you create a content filtering profile.

3. Modify the content filtering profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Content Filtering Profiles page. A confirmation message appears, indicating the status of the edit operation.

Cloning Content Filtering Profiles

Cloning enables you to easily create a new content filtering profile based on an existing one.

To clone a content filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select the content filtering profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Content Filtering Profiles page appears, displaying the same fields that are presented when you create a content filtering profile.

3. Modify the content filtering profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Content Filtering Profiles page. A confirmation message appears, indicating the status of the clone operation.

Deleting Content Filtering Profiles

Before deleting a content filtering profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete a content filtering profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more content filtering profiles:

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select one or more content filtering profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete Profile**.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected content filtering profiles.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

| [Creating Content Filtering Profiles](#) | 552

About the URL Patterns Page

To access this page, select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

Use this page to view, create, edit, clone, and delete URL patterns. A URL pattern contains a list of URLs.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a URL pattern—See [“Creating URL Patterns” on page 559](#).
- Edit, clone, or delete a URL pattern—See [“Editing, Cloning, and Deleting URL Patterns” on page 560](#).
- Clear the selected URL patterns—Click **Clear All Selections** to clear any URL patterns that you might have selected.
- View the details of a URL pattern—Select the URL pattern for which you want to view the details and from the More or right-click menu, select **Detailed View**. The URL Pattern Details page appears displaying the fields shown in [Table 169 on page 558](#).
- Search for URL patterns using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 169 on page 558](#) describes the fields on the URL Patterns page.

Table 169: URL Patterns Page Fields

Field	Description
Name	Name of the URL pattern.
URLs	List of URLs in the URL pattern.
Description	Description of the URL pattern.

RELATED DOCUMENTATION

[About the URL Categories Page](#) | [562](#)

Creating URL Patterns

Use this page to create URL patterns. You can also assign URL patterns to a URL category.

To create a URL pattern:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears.

2. Click the add icon (+) to create a URL pattern.

The Create URL Patterns page is displayed.

3. Complete the configuration according to the guidelines provided in [Table 170 on page 559](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

A new URL pattern is created and you are returned to the URL Patterns page.

Table 170: Create URL Patterns Settings

Settings	Guidelines
Name	Enter a unique name for the URL pattern. The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 29 characters.
Description	Enter a description for the URL pattern. The maximum length is 255 characters.
URL Category	Select the URL category to which you want to assign the URL pattern. Alternatively, click Create New URL Category to create a URL category, enter the URL category name in the text box, and click Save to assign the URL pattern to the new category.

Table 170: Create URL Patterns Settings (continued)

Settings	Guidelines
Add URLs	<p>Enter one or more URLs (separated by commas) in the text box, and click Add. The URLs are displayed in the URL List table.</p> <p>NOTE:</p> <ul style="list-style-type: none">• The following wildcard characters are supported:<ul style="list-style-type: none">• asterisk (*)• period (.)• square brackets ([])• question mark (?)• Precede all wildcard characters with http://.• The asterisk (*) can only be used at the beginning of a URL and must be followed by a period (.).• The question mark (?) can only be used at the end of a URL.• The following are examples of wildcard syntaxes that are supported: http://*.example.net, http://www.example.ne?, and http://www.example.n??.• The following are examples of wildcard syntaxes that are not supported: *.example.???, http://*example.net, http://?, and www.example.ne?.

RELATED DOCUMENTATION

| [Creating URL Categories](#) | 563

Editing, Cloning, and Deleting URL Patterns

IN THIS SECTION

- [Editing URL Patterns](#) | 561
- [Cloning URL Patterns](#) | 561
- [Deleting URL Patterns](#) | 562

You can edit, clone, and delete URL patterns from the URL Patterns page. This topic has the following sections:

Editing URL Patterns

To modify the parameters configured for a URL pattern:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select the URL pattern that you want to edit and click the edit icon (pencil). Alternatively, right-click a pattern and select **Edit URL Patterns**.

The Edit URL Patterns page appears, displaying the same fields that are presented when you create a URL pattern.

3. Modify the URL pattern fields as needed.

4. Click **OK** to save your changes.

You are taken to the URL Patterns page. A confirmation message appears, indicating the status of the edit operation.

Cloning URL Patterns

Cloning enables you to easily create a new URL pattern based on an existing one.

To clone a URL pattern:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select the URL pattern that you want to clone and then select **More > Clone**. Alternatively, right-click a pattern and select **Clone**.

The Clone URL Patterns page appears, displaying the same fields that are presented when you create a URL pattern.

3. Modify the URL pattern fields as needed.

4. Click **OK** to save your changes.

You are taken to the URL Patterns page. A confirmation message appears, indicating the status of the clone operation.

Deleting URL Patterns

Before deleting a URL pattern, ensure that the URL pattern is not referenced in any UTM profiles that are, in turn, used in firewall policy intents or in URL categories referenced in the UTM settings. If you try to delete such a URL pattern, an error message is displayed.

To delete one or more URL patterns:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select one or more URL patterns that you want to delete and click the delete icon (X). Alternatively, right-click a pattern and select **Delete URL Pattern**.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected URL patterns.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

| [Creating URL Patterns](#) | 559

About the URL Categories Page

To access this page, select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

Use this page to view, create, edit, clone, and delete URL categories. A URL category is a list of URL patterns grouped under a single title.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a URL category—See [“Creating URL Categories”](#) on page 563.
- Edit, clone, or delete a URL category—See [“Editing, Cloning, and Deleting URL Categories”](#) on page 565.
- Clear the selected URL categories—Click **Clear All Selections** to clear any URL categories that you might have selected.

- View the details of a URL category—Select the URL category for which you want to view the details and from the More or right-click menu, select **Detailed View**. The URL Category Details page appears, displaying the details of the selected URL category; see [Table 171 on page 563](#) for an explanation of the fields.
- Search for URL categories by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 171 on page 563](#) describes the fields on the URL Categories page.

Table 171: URL Categories Page Fields

Field	Description
Name	Name of the URL category.
URL Patterns	List of URL patterns in the URL category.
Definition Type	Indicates the type of URL category: <ul style="list-style-type: none">• Predefined—URL categories that are loaded by default.• Custom—URL categories that are created by the user.
Description	Description of the URL category.

RELATED DOCUMENTATION

| [About the URL Patterns Page](#) | 558

Creating URL Categories

Use this page to create URL categories. A URL category is a list of URL patterns grouped under a single title.

To create a URL category:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears.

2. Click the add icon (+) to create a URL category.

The Create URL Categories page is displayed.

3. Complete the configuration according to the guidelines provided in [Table 172 on page 564](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

A new URL category is created and you are returned to the URL Categories page.

Table 172: Create URL Categories Settings

Settings	Guidelines
Name	<p>Enter a unique name for the URL category.</p> <p>The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 59 characters.</p>
Description	<p>Enter a description for the URL pattern. The maximum length is 255 characters.</p>
URL Patterns	<p>Select one or more URL patterns in the Available column and click the forward arrow to confirm your selection. The selected URL patterns are displayed in the Selected column.</p> <p>Alternatively, click Create a New Pattern to create a URL pattern and assign it to the URL category. The Create URL Patterns page appears. For more information, see “Creating URL Patterns” on page 559</p> <p>NOTE: You must select at least one URL pattern.</p>

RELATED DOCUMENTATION

| [Editing, Cloning, and Deleting URL Categories](#) | 565

Editing, Cloning, and Deleting URL Categories

IN THIS SECTION

- [Editing URL Categories | 565](#)
- [Cloning URL Categories | 565](#)
- [Deleting URL Categories | 566](#)

You can edit, clone, and delete URL categories from the URL Categories page. This topic has the following sections:

Editing URL Categories

To modify the parameters configured for a URL category:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears, displaying the existing URL categories.

2. Select the URL category that you want to edit and click the edit icon (pencil). Alternatively, right-click a category and select **Edit URL Categories**.

The Edit URL Categories page appears, displaying the same fields that are presented when you create a URL category.

3. Modify the URL category fields as needed.

4. Click **OK** to save your changes.

You are taken to the URL Categories page. A confirmation message appears, indicating the status of the edit operation.

Cloning URL Categories

Cloning enables you to easily create a new URL category based on an existing one.

To clone a URL category:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears, displaying the existing URL categories.

2. Select the URL category that you want to clone and then select **More > Clone**. Alternatively, right-click a category and select **Clone**.

The Clone URL Categories page appears, displaying the same fields that are presented when you create a URL category.

3. Modify the URL category fields as needed.

4. Click **OK** to save your changes.

You are taken to the URL Categories page. A confirmation message appears, indicating the status of the clone operation.

Deleting URL Categories

Before deleting a URL category, ensure that the URL category is not referenced in any UTM profiles that are, in turn, used in firewall policy intents or in the UTM settings. If you try to delete such a URL category, an error message is displayed.

To delete one or more URL categories:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears, displaying the existing URL categories.

2. Select one or more URL categories that you want to delete and click the delete icon (X). Alternatively, right-click a category and select **Delete URL Category**.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected URL categories.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

| [Creating URL Categories](#) | 563

Managing SLA Profiles and SD-WAN Policies

IN THIS CHAPTER

- [Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)
- [About the SD-WAN Policy Page | 573](#)
- [Creating SD-WAN Policy Intents | 575](#)
- [Editing and Deleting SD-WAN Policy Intents | 583](#)
- [Application Quality of Experience Overview | 584](#)
- [Configure and Monitor Application Quality of Experience | 586](#)
- [About the SLA-Based Steering Profiles Page | 587](#)
- [Adding SLA-Based Steering Profiles | 591](#)
- [Editing and Deleting SLA-Based Steering Profiles | 598](#)
- [About the Path-Based Steering Profiles Page | 600](#)
- [Adding Path-Based Steering Profiles | 602](#)
- [Editing and Deleting Path-Based Steering Profiles | 604](#)
- [Breakout and Breakout Profiles Overview | 606](#)
- [About the Breakout Profiles Page | 609](#)
- [Adding Breakout Profiles | 614](#)
- [Adding Cloud Breakout Settings | 616](#)
- [Assigning Cloud Breakout Settings to Sites | 620](#)
- [Detaching Cloud Breakout Settings from Sites | 622](#)
- [Editing Breakout Profiles and Cloud Breakout Settings | 623](#)
- [Deleting Breakout Profiles and Cloud Breakout Settings | 625](#)
- [Configuring Breakout on SD-WAN Sites | 626](#)

Traffic Steering Profiles and SD-WAN Policies Overview

IN THIS SECTION

- [Traffic Steering Profiles | 568](#)
- [SD-WAN Policies | 571](#)

Contrail Service Orchestration (CSO) enables you to create traffic steering profiles and map them to software-defined WAN (SD-WAN) policies for traffic management.

Traffic Steering Profiles

Traffic steering profiles are created for applications or groups of applications for all tenants. Traffic-based steering profiles are categorized as follows:

- **SLA profiles** are created for applications or groups of applications for all tenants. **SLA-Based Steering Profiles**—An SLA-based steering profile consists of a set of configurable constraints such as SLA configuration, SLA threshold, SLA parameters, path selection criteria, Class of Service, and upstream and downstream data rates.

NOTE: The Secure SD-WAN Essentials service does not support SLA-based steering profiles.

- **Path-Based Steering Profiles**—A path-based steering profile consists of a set of configurable constraints such as path preference, traffic type profiles, and upstream and downstream data rates.
- **Breakout Profiles**—A breakout profile consists of set of configurable constraints such as type of breakout, traffic type profiles, path preference, and upstream and downstream data rates. A cloud breakout profile is added by Contrail Service Orchestration (CSO) by default.

[Table 173 on page 569](#), [Table 174 on page 570](#) and [Table 175 on page 570](#) lists the categories of configurable constraints that are defined in an SLA profile.

Table 173: SLA Profile Categories

Category	Description
SLA profile parameters	<p>You can define one or more than one of the following SLA profile parameters:</p> <ul style="list-style-type: none"> • SLA Configuration—Whether to use recommended or custom values for the SLA threshold and SLA parameters. • SLA Threshold—Whether to use, liberal, baseline, or conservative settings for the threshold. • SLA parameters: <ul style="list-style-type: none"> • Packet loss—Percentage of data packets dropped by the network to manage congestion. • RTT—Target round-trip time (RTT) for the SLA profile. • Jitter—Difference between the maximum and minimum round-trip times (in ms) of a packet of data.
Path preference and failover	<p>Paths are the WAN links to be used for the SLA profile. You can select MPLS, Internet, or any link as the preferred path. MPLS is more latency-sensitive than Internet.</p> <p>You can trigger the path failover criteria when any of the SLA parameters is violated, or when all the SLA parameters are violated.</p>
Class of service	<p>Class of service (CoS) provides different levels of service assurances to various forms of traffic. CoS enables you to divide traffic into classes and offer an assured service level for each class. The classes of service listed in increasing order of priority and sensitivity to latency are best effort, voice, interactive video, streaming audio or video, control, and business essential. The default CoS is voice.</p>
Rate limiters	<p>Rate limiters are defined for traffic shaping and efficient bandwidth utilization. You can define the following rate limiters:</p> <ul style="list-style-type: none"> • Maximum upstream and downstream rates—The maximum upstream and downstream rate for all applications associated with the SLA profile. • Maximum upstream and downstream burst sizes—The maximum size of a steady stream of traffic sent at average rates that exceed the upstream and downstream rate limits for short periods.

NOTE: You must define at least one of the SLA parameters or path preference. You cannot leave both path preference and SLA parameters fields blank at the same time.

Table 174: Path-Based Profile Categories

Category	Description
Path preference	Paths are the WAN links to be used for the SLA profile. You can select an MPLS or Internet link as the preferred path. MPLS is more latency-sensitive than Internet.
Class of service	Class of service (CoS) provides different levels of service assurances to various forms of traffic. CoS enables you to divide traffic into classes and offer an assured service level for each class. The classes of service listed in increasing order of priority and sensitivity to latency are best effort, voice, interactive video, streaming audio or video, control, and business essential. The default CoS is voice.
Rate limiters	<p>Rate limiters are defined for traffic shaping and efficient bandwidth utilization. You can define the following rate limiters:</p> <ul style="list-style-type: none"> • Maximum upstream and downstream rates—The maximum upstream and downstream rate for all applications associated with the SLA profile. • Maximum upstream and downstream burst sizes—The maximum size of a steady stream of traffic sent at average rates that exceed the upstream and downstream rate limits for short periods.

Table 175: Breakout Profile Categories

Category	Description
Type	<p>The type of breakout profile that you want to add:</p> <ul style="list-style-type: none"> • Local Breakout (Underlay)—Select this option if you want traffic to break out locally (on the underlay) from the site. • Backhaul—Select this option if you want traffic to break out through a hub or a enterprise hub (if configured). • Local Breakout (Cloud)—Select to break out traffic through a cloud-based security platform. Currently, Zscaler is the only cloud-based security platform supported.
Traffic Type Profile	The traffic type profile to apply class of service parameters to the breakout traffic. You can select only a traffic type profile that is enabled.
Preferred Path	<p>The preferred path (MPLS, Internet, or Any) to be used for breaking out the traffic.</p> <p>If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.</p> <p>If you specify that any path can be used, then there is no preference and all breakout-enabled links are used in a load-balancing mode.</p>

Table 175: Breakout Profile Categories (*continued*)

Category	Description
Rate Limiting	<p>Rate limiting of breakout traffic for cacheable applications. By default, rate limiting is disabled.</p> <p>If you enable rate limiting, you must specify the upstream and downstream parameters, and the loss priority.</p>
Upstream Rate	The maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
Upstream Burst Size	The maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the upstream rate limit for short periods.
Downstream Rate	The maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
Downstream Burst Size	The maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the downstream rate limit for short periods.
Loss Priority	Loss priority based on which packets are dropped or retained when network congestion occurs. Packet drops are most likely when the loss priority is High and least likely when the loss priority is Low.

SD-WAN Policies

SD-WAN policy intents help in optimum utilization of the WAN links and efficient load distribution of traffic. SD-WAN policy intents are applied to source endpoints (such as sites and departments) and destination endpoints (applications or application groups) and can be defined for site-to-site traffic (by using SLA profiles) or for breakout traffic (by using breakout profiles).

Policy intents consist of the following parameters:

- **Source**—A source endpoint that you can choose from a list of sites, site groups, and departments or a combination of all of these. The SD-WAN policy intent is applied to the selected source endpoint.
- **Destination**—A destination endpoint that you can choose from a list of applications and predefined or custom application groups. You can select a maximum of 32 applications or application groups as destination endpoints. The SD-WAN policy intent is applied to the selected destination endpoint.

Applications are classified into the following categories:

- **Cacheable applications**, which refer to applications or application groups that are stored in the application cache when they are recognized by the device. After they are stored in the application cache, subsequent sessions are routed directly through the correct WAN link.

- Non-cacheable applications, which refer to applications or application groups that are not stored in the application cache and all sessions are first routed through the default path, and then routed to the correct WAN link based on the SD-WAN policy.
- **Traffic Steering Profile**—Depending on whether you want to apply the policy intent to site-to-site traffic or breakout traffic, you can associate the traffic steering profile with the policy intent. The following options are available:
 - SLA-based steering profile— Applicable for site-to-site traffic (Not applicable to the Secure SD-WAN Essentials service.)
 - Path-based steering profile— Applicable for site-to-site traffic
 - Breakout profile—Applicable for breakout traffic (local, central, or cloud).
- **Intent name**—A unique name for the SD-WAN policy intent.

SD-WAN supports advanced policy-based routing (APBR). APBR enables you to dynamically define the routing behavior of the SD-WAN network based on applications. Dynamic application-based routing makes it possible to define policies and to switch WAN links on the fly based on the application's defined SLA parameters. The APBR mechanism classifies sessions based on applications and application signatures and uses policy intents to identify the best possible route for the application. When the best possible route does not meet the application's defined SLA requirements, the SD-WAN network finds the next best possible route to meet SLA requirements.

For example, consider an application in a site. If you want the application group to use custom throughput, latency, or jitter, you can create an SLA profile with these custom values. You can then create an intent and configure the intent with the application and apply the custom SLA profile. When the intent is deployed, CSO determines the best suited WAN link to route traffic based in the application. If the WAN link fails to meet SLA requirements in runtime, the SD-WAN network switches WAN links to the next best suited path.

On the basis of the configured traffic-based steering profile constraints, you can categorize SD-WAN policies into three types:

- **Path-based steering policy**—If only the path preference is defined and none of the SLA parameters are defined in the SLA profile, then the policy is called a path-based steering policy. In path-based steering profile, you can define the path (MPLS or Internet) that must be used for a given traffic type profile. You cannot configure SLA parameters or path failover criteria for a path-based steering profile. The traffic type profile must be in enabled state in order to be used in any profile.
- **SLA-based steering policy**—If one or more SLA parameters in the SLA profile are defined, then the policy is called an SLA-based steering policy. In an SLA-based steering profile, each profile is associated with a traffic type profile and tracks the SLA parameters such as packet loss, Jitter and RTT. The traffic type profile must be in enabled state in order to be used in any profile. Based on your requirements, you can choose the recommended SLA threshold or enter custom SLA threshold for the traffic type profile. You can even set the path preference (Any, MPLS, or Internet) to switch traffic from one WAN interface to another based on the path failover criteria.

When an intent is deployed on a site, if the WAN link chosen by the SD-WAN network does not meet the SLA requirements and the network performance deteriorates, then the site switches WAN links to meet the SLA requirements. The link switching is recorded as an SD-WAN event and displayed in the SD-WAN Events page in the customer portal and the *Tenant_name* SLA Performance pages in the administration and customer portals.

- **Breakout policy**—If local breakout, central breakout, or cloud breakout parameters are defined, then the policy is called a breakout policy.

RELATED DOCUMENTATION

[About the SD-WAN Policy Page | 573](#)

[Breakout and Breakout Profiles Overview | 606](#)

[SD-WAN Events Overview | 853](#)

About the SD-WAN Policy Page

To access this page, select **Configuration > SD-WAN > SD-WAN Policy** in the Customer Portal.

SD-WAN policy intents help in optimum utilization of the WAN links and efficient load distribution of traffic. SD-WAN policy intents are applied to source endpoints (such as sites and departments) and destination endpoints (applications or application groups) and can be defined for site-to-site traffic (by using SLA profiles) or for breakout traffic (by using breakout profiles).

NOTE: When packets match more than one policy intents, CSO prefers the policy with more specific intent rules over the policy with broader intent rules to help steer traffic. For example, consider that you have one policy with the application WIKIPEDIA and another with the application HTTPS deployed. In this case, any traffic destined to <https://wikipedia.org> takes the path defined for the policy with the application WIKIPEDIA as it is a more specific parameter.

You can use the SD-WAN Policy page to view, create, edit, and deploy SD-WAN policy intents. SD-WAN policy intents use SLA profiles for traffic management. SD-WAN policies help in optimum utilization of the WAN links and efficient distribution of traffic. Every tenant has an SD-WAN policy and intents are created in the SD-WAN policy.

Tasks You Can Perform

You can perform the following tasks from this page:

- View existing SD-WAN policy intents. CSO provides pre-defined SD-WAN policy intents for the tenants. See [Table 177 on page 574](#).

NOTE: The pre-defined SD-WAN policy intents are available for the tenants only if the SP administrator has the downloaded the signature database prior to creating the tenants.

- Create SD-WAN policy intents. See [“Creating SD-WAN Policy Intents” on page 575](#).
- Edit or delete SD-WAN policy intents. See [“Editing and Deleting SD-WAN Policy Intents” on page 583](#).
- Deploy SD-WAN policy intents. See [“Deploying Policies” on page 742](#).
- View the number of undeployed SD-WAN policy intents.
- Search for SD-WAN policy intents using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

[Table 176 on page 574](#) describes the fields on the SD-WAN Policy page.

Table 176: Fields on the SD-WAN Policy Page

Field	Description
Name	Displays the name of the SD-WAN policy intent.
Source	Displays the source endpoints that are configured for the policy intents. A source endpoint is chosen from sites, site groups, and departments or a combination of all of these to which the policy intent is applied.
Destination	Displays the application destination endpoints that are configured for the policy intents. An application destination endpoint is chosen from a list of applications and predefined or custom application groups to which the policy intent is applied.
Traffic Steering Profile	Displays the breakout profile or the SLA profile associated with the policy intent.

Table 177: Pre-defined SD-WAN Policies

SD-WAN Policy Name	Applicable Sites	Application	Traffic Steering Profile
System-1	All Sites	CSO-Collaboration	CSO-AV
System-2	All Sites	CSO-Security	CSO-Sec

Table 177: Pre-defined SD-WAN Policies (*continued*)

SD-WAN Policy Name	Applicable Sites	Application	Traffic Steering Profile
System-3	All Sites	CSO-Collaboration	CSO-Email
System-4	All Sites	CSO-Productivity	CSO-Productive
System-5	All Sites	CSO-File-Share	CSO-FileShare

RELATED DOCUMENTATION

[Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)

[Creating SD-WAN Policy Intents | 575](#)

[Editing and Deleting SD-WAN Policy Intents | 583](#)

Creating SD-WAN Policy Intents

You can create policy intents for SD-WAN policies from the **SD-WAN Policy** page.

To create an SD-WAN policy intent:

1. Select **Configuration > SD-WAN > SD-WAN Policy** in Customer Portal.

The SD-WAN Policy page appears.

2. Click the add icon (+).


The options to create policy intents appear inline on the SD-WAN Policy page.

3. Enter the policy intent information according to the guidelines provided in [Table 178 on page 577](#).

4. Click **Save** to create the policy intent.

The SD-WAN policy intent is saved and a confirmation message is displayed.

NOTE: After the policy intent is created, you must deploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications. When an SD-WAN policy intent is created, the Undeployed field is incremented by one indicating that intents are pending deployment.



NOTE: The SD-WAN Essentials service does not support department-level policy intents or SLA-based steering profiles.

Table 178: Create SD-WAN Policy Intent Settings

Field	Guidelines
Source	

Table 178: Create SD-WAN Policy Intent Settings (*continued*)

Field	Guidelines
	<p>You can select the source endpoints in one of the following ways:</p> <p>Click the + box under the Source field and then,</p> <ul style="list-style-type: none"> • Select source endpoints from the displayed list of IP addresses or IP address range, departments, sites, or site groups, or a combination of these. Click the source endpoints to select them. <p>NOTE: If you are selecting an IP address, you must also select a specific site (not All Sites) or department (or both).</p> <ul style="list-style-type: none"> • Select the source endpoints from the complete list of IP addresses or IP address range, departments, sites, and site groups. <p>To view the complete list of IP addresses or IP address range, departments, sites, and site groups.</p> <ol style="list-style-type: none"> 1. Click View more results. The complete list of departments, sites, and site groups is displayed in the End Points pane on the right. 2. (Optional) Hover over a department or site group and click the edit icon to edit the department or site group. You cannot edit a site. 3. Click the add icon (+) to select the endpoint. <ul style="list-style-type: none"> • Start typing the endpoint name in the Source field. As you type, the filtered list of source endpoints is displayed. You can click the displayed source endpoint to select it. • Create IP addresses, site groups, or departments to select the source endpoint from the newly created site group or department. <p>To create addresses, site groups, or departments:</p> <ol style="list-style-type: none"> 1. Click anywhere within the Source field. 2. Click the lesser-than icon (<) on the right. <p>The list of available departments, sites, and site groups is displayed in the End Points pane on the right.</p> <ol style="list-style-type: none"> 3. (Optional) To view more information about a source endpoint, hover over the endpoint click the details icon. 4. Click the add icon (+) on the top right of the pane. 5. Click Address, Department, or Site Group as needed. The Add Department page or

Table 178: Create SD-WAN Policy Intent Settings (continued)

Field	Guidelines
	<p>Create Site Group page appears based on your selection. See “Creating Addresses or Address Groups” on page 753, “Add a Department” on page 783, and “Creating Site Groups” on page 217 for information about creating the endpoints.</p> <p>6. Click the check mark icon (✓) if you want to save the department or site group to the policy intent.</p> <p>Alternatively, if you want to discard your updates, click Cancel instead.</p>

Table 178: Create SD-WAN Policy Intent Settings (continued)

Field	Guidelines
Destination/Application	

Table 178: Create SD-WAN Policy Intent Settings (*continued*)

Field	Guidelines
	<p>You can select the application endpoints in one of the following ways:</p> <p>NOTE: You can choose Any in the Applications field, only if the selected sites were upgraded to CSO 6.1.0 or later versions.</p> <p>Click in the + box under the Destination/Application field and then,</p> <ul style="list-style-type: none"> • Select Destination/Application endpoints from the displayed list of addresses, services (Layer 4 applications), applications and application groups (Layer 7 application). Click the endpoints to select them. <p>NOTE: Layer 4 applications (services) and Layer 7 applications (applications or application groups) are mutually exclusive. You can choose either the services or the applications in the same intent.</p> <ul style="list-style-type: none"> • Select the Destination/Application endpoints from the complete list of applications and application groups. <p>To view the complete list of applications and applications groups.</p> <ol style="list-style-type: none"> 1. Click View more results. The complete list of applications and applications groups is displayed in the End Points pane on the right. 2. (Optional) Hover over an application group and click the edit icon to edit the application group. 3. (Optional) Hover over an application and click the details icon to view details about the application. 4. Click the add icon (+) to select the endpoint. <ul style="list-style-type: none"> • Start typing the endpoint name in the Destination/Application field. As you type, the filtered list of source endpoints is displayed. • Create custom Destination/Application endpoints and select them. <p>To create a Destination/Application endpoint:</p> <ol style="list-style-type: none"> 1. Click anywhere within the Application field. 2. Click the lesser-than icon (<) on the right. <p>The list of available applications, departments, sites, and site groups is displayed in the End Points pane on the right.</p> <ol style="list-style-type: none"> 3. Click the add icon (+) on the top right of the pane.

Table 178: Create SD-WAN Policy Intent Settings (*continued*)

Field	Guidelines
	<p>4. Click Application > Application Signature/Application Signature Group, Address, or Service. See “Creating Addresses or Address Groups” on page 753, “Creating Services and Service Groups” on page 759, “Adding Application Signatures” on page 772, “Adding Application Signature Groups” on page 779 for more information about creating the endpoints.</p> <p>5. Click the check mark icon (✓) if you want to save the application signature group to the policy intent.</p> <p>Alternatively, if you want to discard your updates, click Cancel instead.</p>
Traffic Steering Profile	<p>Click the + field under the Traffic Steering Profile field and then select a breakout profile, SLA-based profile, or a path-based profile to apply to the source and application endpoints. You can select the profile in one of the following ways:</p> <ul style="list-style-type: none"> • Select the breakout profile, SLA-based profile, or the path-based profile from the displayed list of profiles. Click the profile to select it. • Select the profile from the complete list of breakout, SLA-based, or path-based profiles: To view the complete list of breakout, SLA-based, or path-based profiles. <ol style="list-style-type: none"> 1. Click View more results. The complete list of profiles is displayed in the End Points pane on the right. 2. Click the add icon (+) to select the profile. • Select the profile by creating a custom SLA-based, path-based, or breakout profile: <ul style="list-style-type: none"> • To create a traffic steering profile: <ol style="list-style-type: none"> 1. Click anywhere within the Traffic Steering Profile field. 2. Click the lesser-than icon (<) on the right. 3. Click the add icon (+) on the top right of the pane and select SLA-Based Steering Profiles, Breakout Profiles, or Path-Based Steering Profiles. <p>For more information about creating the traffic steering profiles, see “Adding Breakout Profiles” on page 614, “Adding SLA-Based Steering Profiles” on page 591, and “Adding Path-Based Steering Profiles” on page 602.</p>
Options	
Name	Enter a name for the policy intent.

Table 178: Create SD-WAN Policy Intent Settings (continued)

Field	Guidelines
Description	Enter a description for the policy intent.

RELATED DOCUMENTATION

Traffic Steering Profiles and SD-WAN Policies Overview		568
About the SD-WAN Policy Page		573
Editing and Deleting SD-WAN Policy Intents		583
Deploying Policies		742

Editing and Deleting SD-WAN Policy Intents

IN THIS SECTION

- [Editing SD-WAN Policy Intents](#) | [583](#)
- [Deleting SD-WAN Policy Intents](#) | [584](#)

You can edit or delete SD-WAN policy intents from the SD-WAN Policy page.

Editing SD-WAN Policy Intents

You can edit SD-WAN policy intents from the SD-WAN Policy page.

To edit an SD-WAN policy intent:

1. Hover over the SD-WAN policy intent that you want to edit, and then click the edit icon that appears on the right side of the policy intent.

The options to create policy intents appear within the SD-WAN Policy page showing the same options that you see when you create a new SD-WAN policy intent.
2. Modify the parameters according to the guidelines provided in [“Creating SD-WAN Policy Intents” on page 575](#).

3. Click **Save** to save your changes.

Alternatively, click **Cancel** to discard your changes.

NOTE: After you modify an SD-WAN policy intent, you must redeploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications.

Deleting SD-WAN Policy Intents

If an SD-WAN intent is no longer needed, you can delete the SD-WAN policy intent from the SD-WAN Policy page.

To delete one or more SD-WAN policy intents:

1. Select one or more policy intents that you want to delete and click the delete icon (trash can).

A page appears asking you to confirm the delete operation.

2. Click **Yes** to confirm that you want to delete the selected policy intents.

A confirmation message appears indicating the status of the delete operation.

NOTE: After you delete one or more SD-WAN policy intents, you must redeploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications.

RELATED DOCUMENTATION

[Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)

[About the SD-WAN Policy Page | 573](#)

[Creating SD-WAN Policy Intents | 575](#)

Application Quality of Experience Overview

IN THIS SECTION

- [Benefits of Application Quality of Experience | 586](#)

Contrail Service Orchestration (CSO) supports Application Quality of Experience (AppQoE) that enables you to effectively prioritize, segregate, and route business-critical application traffic without compromising performance or availability.

AppQoE utilizes the capabilities of two application security services:

- Application identification (AppID) to identify specific applications in your network.
- Advanced policy-based routing (APBR) to specify a path for the application traffic.

AppQoE-enabled devices perform service-level agreement (SLA) measurements across the available WAN links, and then dynamically map the application traffic to the path that best serves the application's SLA requirement.

NOTE: AppQoE is applicable only for SD-WAN sites.

AppQoE is supported on the following devices in both hub-and-spoke and full mesh topologies:

- vSRX instances
- SRX300 series
- SRX550M
- SRX1500
- SRX4100
- SRX4200

You can configure an AppQoE between two SRX Series device endpoints (book-ended) when both the devices run the same version of Junos OS.

CSO pushes the SLA parameters, path selection parameters and related configuration to the device and the device monitors the links for SLA violation. If there is a violation, the device switches the link and generates **APPQOE_(APP)_SLA_METRIC_VIOLATION** and **APPQOE_BEST_PATH_SELECTED** system log messages. The device also aggregates and averages the SLA metrics, and generates periodic **APPQOE_APP_PASSIVE_SLA_METRIC_REPORT** system log messages.

AppQoE measures the application performance across multiple links by collecting real-time data by continuously monitoring application traffic and identifying any network or device issues by sending active and passive probes. To monitor the SLA compliance of the link on which the application traffic is sent, the Customer Premises Equipment (CPE) device sends inline probes (called passive probes) along with the application traffic. Additionally, to identify the best available link for an application if the active link fails to meet the SLA criteria, the CPE constantly monitors and collects the SLA compliance data for the other available links by sending probes (called active probes) over the links. The active probes are sent based on the probe parameters that you configure in the application traffic type profile.

The CPE device switches links at the application level, which means that only the traffic corresponding to the application that reported the SLA violation is moved to a link that meets the specified SLA. Traffic for the remaining applications remain on the same link until those applications report an SLA violation.

You can configure traffic type profiles to specify the class of service (CoS) and probe parameters for each traffic type. When you add a steering profile (SLA-based or path-based), you specify the SLA parameters and SLA sampling criteria, and link the steering profile with a traffic type profile. The steering profile is then linked to an SD-WAN policy intent and the SD-WAN policy is deployed to enable AppQoE.

From the Application SLA Performance (**Monitor > Application SLA Performance**) page, you can view the application-level SLA performance information and whether AppQoE is enabled. You can also view applications-level SLA performance details such as packet loss, round-trip time (RTT), jitter metric, throughput, latency metric, and the number of probes.

For more information on the AppQoE workflow, see [“Configure and Monitor Application Quality of Experience” on page 586](#).

Benefits of Application Quality of Experience

- Enables cost-effective QoE by real-time monitoring of application traffic, which provides a consistent and predictable level of service.
- Improves the user experience at the application level by ensuring that the application data is sent over the most SLA-compliant link.

RELATED DOCUMENTATION

| [Application Quality of Experience](#)

Configure and Monitor Application Quality of Experience

Application Quality of Experience (AppQoE) improves the user experience by constantly monitoring the class of service (CoS) parameters and service-level agreement (SLA) compliance of the available WAN links, ensuring that the application data is sent over the most SLA-compliant link. For more information, see [“Application Quality of Experience Overview” on page 584](#).

NOTE: Ensure that Service Provider (SP) administrator has enabled the required traffic type profiles.

As a tenant administrator user, to configure and monitor AppQoE in Customer Portal:

1. Add an SLA-based steering profile or a path-based steering profile and associate a traffic type profile with the added steering profile. For more information, see [“Adding SLA-Based Steering Profiles” on page 591](#) or [“Adding Path-Based Steering Profiles” on page 602](#).
2. Add an SD-WAN policy intent that references to the steering profile you added previously. For more information, see [“Creating SD-WAN Policy Intents” on page 575](#).

NOTE: Before you deploy an SD-WAN policy, ensure that you have added one or more SD-WAN sites. For more information, see [“About the Site Management Page” on page 68](#).

3. Deploy the SD-WAN policy on one or more SD-WAN sites to enable AppQoE. For more information, see [“Deploying Policies” on page 742](#).
4. View the SLA performance details of all the sites in a tenant on the Application SLA Performance page (**Monitor > Application SLA Performance**). For more information, see [“About the SLA Performance of a Single Tenant Page” on page 856](#).

RELATED DOCUMENTATION

[About the SLA-Based Steering Profiles Page | 587](#)

[About the SD-WAN Policy Page | 573](#)

About the SLA-Based Steering Profiles Page

To access this page, select **Configuration > SD-WAN > SLA-Based Steering Profiles** in the Customer Portal.

You can use the SLA-Based Steering Profiles page to view information about service-level agreement (SLA)-based steering for the tenant profile in which you are logged in.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of SLA profiles for the tenants.
- Add an SLA-based steering profile for the tenant. See [“Adding SLA-Based Steering Profiles” on page 591](#).

- Edit or delete an SLA-based steering profile. See [“Editing and Deleting SLA-Based Steering Profiles” on page 598](#).
- Show or hide columns that contain information about SLA-based steering profiles. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for SLA-based steering profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

[Table 179 on page 588](#) shows the descriptions of the fields on the SLA-Based Steering Profiles page.

Table 179: Fields on the SLA-Based Steering Profiles Page

Field	Description	Displayed On
Name	Name of the SLA-based steering profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
Priority	Priority of the SLA-based steering profile. A value zero (0) indicates lower priority and one (1) indicates highest priority.	Detail for <i>SLA-Profile-Name</i> pane
Traffic Type Profile	Indicates the traffic type profile associated with the SLA-based steering profile. <ul style="list-style-type: none"> • VOICE-VIDEO • HIGH_PRIORITY_VIDEO • HOSTED_AV • PREMIUM_INTERNET • INTERNET 	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
Packet Loss (%)	Target packet loss for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
Jitter (ms)	Target jitter for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane

Table 179: Fields on the SLA-Based Steering Profiles Page (*continued*)

Field	Description	Displayed On
RTT	Target round-trip time (RTT) for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for <i>SLA-Profile-Name</i> pane
Created By	Name of the user who created the SLA-based steering profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)
Path Preference	The preferred path for the SLA profile. The available options are: <ul style="list-style-type: none"> • MPLS • Internet • Any (default) 	Detail for <i>SLA-Profile-Name</i> pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for <i>SLA-Profile-Name</i> pane
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for <i>SLA-Profile-Name</i> pane
Sampling Period	The sampling period, in milliseconds, for which the SLA violations are counted.	Detail for <i>SLA-Profile-Name</i> pane
Switch Cool-off Period	The waiting period, in milliseconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links.	Detail for <i>SLA-Profile-Name</i> pane
Path Failover Criteria	Indicates the path failover criteria for link switching. Path failover occurs when any (Any)of the SLA parameters is violated or when all (All) the SLA parameters are violated.	Detail for <i>SLA-Profile-Name</i> pane
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the SLA-based steering profile.	Detail for <i>SLA-Profile-Name</i> pane

Table 179: Fields on the SLA-Based Steering Profiles Page (continued)

Field	Description	Displayed On
Maximum Upstream Burst Size	The maximum upstream burst size (in bytes).	Detail for <i>SLA-Profile-Name</i> pane
Maximum Downstream Rate	The maximum downstream rate (in Kbps) for all applications associated with the SLA-based-steering profile.	Detail for <i>SLA-Profile-Name</i> pane
Maximum Downstream Burst Size	The maximum downstream burst size (in bytes).	Detail for <i>SLA-Profile-Name</i> pane

RELATED DOCUMENTATION

| [Traffic Steering Profiles and SD-WAN Policies Overview](#) | 568

Adding SLA-Based Steering Profiles

You can use the Add SLA Profile page to add a new service-level agreement (SLA)-based steering profile, specify the traffic type profile, SLA configuration, SLA threshold, SLA parameters, path selection criteria, and rate limiting parameters for the profile. [Table 180 on page 592](#) lists the SLA-based steering profiles that are tuned for specific application categories and traffic types.

NOTE: Secure SD-WAN Essentials Service does not support SLA-based steering profiles.

Table 180: Predefined SLA-Based Steering Profiles

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-AV	VOICE-VIDEO	CSO_Collaboration_AV	Skype for Business Zoom Video GotoMeeting Jive Jabber Citrix Online WebEx Zoho Meeting Google Hangout Adobe Connect

Table 180: Predefined SLA-Based Steering Profiles (continued)

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-Productivity	PREMIUM-INTERNET	CSO_Productivity	ERP: Salesforce, Oracle, SAP Office365 (including SharePoint) Zendesk HRPayroll Zoho Office Suite Slack Square Concur Adobe Quickbooks Freshbooks Workday Project Management-MS PJ Basecamp Asana
CSO-Security	INTERNET	CSO_Security	Symantec McAfee Sophos Zonealarm Lookout

Table 180: Predefined SLA-Based Steering Profiles (*continued*)

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-Email	PREMIUM-INTERNET	CSO_Collaboration_Email	MS Exchange IMAP POP3 Gmail OWA Yahoo
CSO-FileShare	INTERNET	CSO_File_Share	Box Dropbox Gsuite OneDrive Skype for Business-File Transfer Zoho Share

To add an SLA-based steering profile to the tenant:

1. Select **Configuration > SD-WAN > SLA-Based Steering Profiles**.

The SLA-Based Steering Profiles page appears.

2. Click the add icon (+).

The Add SLA Profile page appears.

3. Enter the SLA profile information according to the guidelines provided in [Table 181 on page 595](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK** to add the SLA profile.

The SLA-Based Steering Profiles page appears with the new SLA profile information. You are returned to the SLA-Based Steering Profiles page and a confirmation message indicating that the SLA-based

steering profile was added is displayed. The page refreshes to display the SLA-based steering profile that you added.

Alternatively, if you want to discard your updates, click **Cancel** instead.

NOTE: After you add an SLA-based steering profile, you must add an SD-WAN policy intent that references the SLA-based steering profile in order to enable site-to-site traffic.

Table 181: Fields on the Add SLA Profile page

Field	Guidelines
<i>General</i>	
Name	Enter a unique string that can contain alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Traffic Type Profile	Choose a traffic type profile to apply the class-of-service configuration and priority to the SLA profile. You can select a traffic type profile only when it is in the Enabled state.
SLA Configuration	Choose one of the following options: <ul style="list-style-type: none"> ● Use Recommended: To use the default SLA threshold and SLA parameters for the SLA-based steering profile. ● Enter Custom: To specify customized values for SLA configuration and SLA parameters for the SLA-based steering profiles.
SLA Threshold	Choose one of the following options: <ul style="list-style-type: none"> ● Liberal—To use a relaxed SLA threshold. ● Baseline—To use the default SLA threshold. ● Conservative—To use a strict SLA threshold.
<i>SLA Parameters</i>	
Packet Loss	Enter the target packet loss (in %) for the SLA-based steering profile. Packet loss is the percentage of data packets dropped by the network to manage congestion.
RTT	Enter the target round-trip time (RTT) for the SLA-based steering profile.
Jitter	Enter the target jitter (in ms) for the SLA-based steering profile. Jitter is the difference between the maximum and minimum round-trip times of a packet of data.

Table 181: Fields on the Add SLA Profile page (continued)

Field	Guidelines
<i>Path Selection Criteria</i>	
Path Preference	<p>Select the preferred WAN link type (MPLS, Internet, or Any) to associate with the SLA profile. Any is the default value.</p> <p>If a WAN link type that matches the preferred path is enabled, then that WAN link type is used for all traffic from the site.</p> <p>If you specify that any path can be used, then there is no preference and all traffic-enabled links are used in a load-balancing mode.</p>
Strict Affinity	<p>This field is displayed only if you select MPLS or Internet as the path preference.</p> <p>Enable the toggle button to use strict link affinity.</p> <p>For strict link affinity, AppQoE ensures that the path selected is always of the preferred link type. If the preferred link does not meet the SLA, then the traffic remains on the preferred link with the status as SLA not met. If multiple links of the preferred link type are available, then the traffic selects the link that has the highest priority and meets the SLA.</p> <p>If the link affinity is not strict and if SLA meeting links belonging to the preferred link type are not available, then AppQoE selects a link outside the preferred link type that meets the SLA requirements. If multiple links meeting the SLA are available, then the traffic switches over to the link with the highest priority. If the traffic switches over to a non-preferred link type, then the traffic automatically reverts to the preferred link when the preferred link recovers and conforms to the SLA.</p>
Path Failover Criteria	<p>Specify the failover criteria to determine how links are switched when the active links fail to meet the SLA criteria. In such cases, the traffic is routed to links that meet SLA criteria.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> ● Does not meet one or more SLA parameters—This triggers the path failover if any of the SLA parameters is violated. ● Does not meet all SLA parameters—This triggers the path failover only when all the SLA parameters are violated.
<i>Advanced Configuration-</i>	
Rate Limiting	

Table 181: Fields on the Add SLA Profile page (continued)

Field	Guidelines
Maximum Upstream Rate	Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps
Maximum Upstream Burst Size	Enter the maximum upstream burst size (in bytes). Range: 1 through 1,342,177,280 bytes
Maximum Downstream Rate	Enter the maximum downstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps
Maximum Downstream Burst Size	Enter the maximum downstream burst size (in bytes). Range: 1 through 1,342,177,280
Loss Priority	Select a loss priority based on which packets can be dropped or retained when network congestion occurs. The chances of a packet getting dropped is the highest when the loss priority is set to High . Other available values are Medium High , Medium Low , and Low .

Real Time Optimized Mode Setting

NOTE: The following fields are applicable only for sites configured with the real-time-optimized SD-WAN mode.

SLA Sampling	
Session-sampling %	Enter the matching percentage of sessions for which you want to run the passive probes.
SLA-violation-count	Enter the number of SLA violations after which you want CSO to switch paths. The range is 1 through 32.
Sampling-period	Enter the sampling period, in seconds, for which the SLA violations are counted. The range is 2 through 60.
Switch-cool-off-period	Enter the waiting period, in seconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links. The range is 5 through 300.

NOTE: If you do not specify the **Switch-cool-off-period** and **SLA-violation-count** parameters, the traffic does not automatically revert to the preferred link when the preferred link comes back online after an SLA violation.

RELATED DOCUMENTATION

[Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)

[About the SLA-Based Steering Profiles Page | 587](#)

[Editing and Deleting SLA-Based Steering Profiles | 598](#)

Editing and Deleting SLA-Based Steering Profiles

IN THIS SECTION

● [Editing an SLA-Based Steering Profile | 598](#)

● [Deleting SLA-Based Steering Profiles | 599](#)

You can use the SLA-Based Steering Profiles page to edit and delete SLA profiles.

NOTE: You cannot edit the predefined SLA-Based steering profiles that are automatically created by Contrail Service Orchestration (CSO).

Editing an SLA-Based Steering Profile

To edit an SLA-based steering profile:

NOTE: If you edit an SLA-based steering profile that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SD-WAN > SLA-Based Steering Profiles**.

The SLA-Based Steering Profiles page appears.

2. Select the SLA-based steering profile that you want to edit, and click the Edit (pencil) icon.

The Edit SLA Profile page appears displaying the same fields that are presented when you add a SLA-based steering profile. For more information, see [“Adding SLA-Based Steering Profiles” on page 591](#).

3. Modify the fields as needed.

NOTE: You cannot edit the SLA-based steering profile name.

4. Click **OK**.

You are returned to the SLA-Based Steering Profiles page. The modifications that you made are saved and a confirmation message is displayed.

Deleting SLA-Based Steering Profiles

You can delete the SLA-based steering profile if they are no longer needed. To delete one or more SLA-based steering profile:

NOTE: You cannot delete an SLA-based steering profile if it is referenced by one or more SD-WAN policy intents.

1. Select **Configuration > SD-WAN > SLA Based Steering Profiles**.

The SLA-Based Steering Profiles page appears.

2. Select the SLA-based steering profiles that you want to delete and click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

3. Click **Yes**.

You are returned to the SLA-Based Steering Profiles page. The selected SLA-based steering profile is deleted and a confirmation message is displayed.

RELATED DOCUMENTATION

[Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)

[About the SLA-Based Steering Profiles Page | 587](#)

[Adding SLA-Based Steering Profiles | 591](#)

About the Path-Based Steering Profiles Page

To access this page, select **Configuration > SD-WAN > Path-Based Steering Profiles** in the Customer Portal.

You can use the Path-Based Steering Profiles page to view information about path profiles for the tenant profile in which you are logged in.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of path-based steering profiles for the tenant.
- Add path-based steering profiles for the tenant. See [“Adding Path-Based Steering Profiles” on page 602](#).
- Edit or delete a path-based steering profile. See [“Editing and Deleting Path-Based Steering Profiles” on page 604](#).
- Show or hide columns that contain information about path-based steering profile. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for path-based steering profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

[Table 182 on page 600](#) shows the descriptions of the fields on the Path-Based Steering Profiles page.

Table 182: Fields on the Path-Based Steering Profiles Page

Field	Description	Displayed on
Name	Name of the path-based-steering profile.	Path-Based Steering Profiles Page (Path Profiles List tab) Detail for <i>Path-Profile-Name</i> pane
Traffic Type Profile	Indicates the traffic type profile associated with the path-based-steering profile. <ul style="list-style-type: none"> • VOICE-VIDEO • HIGH_PRIORITY_VIDEO • HOSTED_AV • PREMIUM_INTERNET • INTERNET 	Path-Based Steering Profiles Page (Path Profiles List tab) Detail for <i>Path-Profile-Name</i> pane

Table 182: Fields on the Path-Based Steering Profiles Page (*continued*)

Field	Description	Displayed on
Path Preference	<p>The preferred path for the SLA profile. The available options are:</p> <ul style="list-style-type: none"> • MPLS • Internet 	<p>Path-Based Steering Profiles Page (Path Profiles List tab)</p> <p>Detail for <i>Path-Profile-Name</i> pane</p>
Created by	The name of the user who created the path profile.	Path-Based Steering Profiles Page (Path Profiles List tab)
Priority	Priority of the path-based steering profile. A value zero (0) indicates lower priority and one (1) indicates highest priority.	Detail for <i>Path-Profile-Name</i> pane
Packet Loss	Target packet loss for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
RTT	Target round-trip time (RTT) for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
Jitter	Target jitter for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for <i>Path-Profile-Name</i> pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for <i>Path-Profile-Name</i> pane
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for <i>Path-Profile-Name</i> pane
Sampling Period	The sampling period, in milliseconds, for which the path-based steering profile violations are counted.	Detail for <i>Path-Profile-Name</i> pane
Switch Cool-off Period	The waiting period, in milliseconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links.	Detail for <i>Path-Profile-Name</i> pane
Path Failover Criteria	Indicates the path failover criteria for link switching. Path failover occurs when any (Any)of the path-based steering profile parameters is violated or when all (All) the path-based steering profile parameters are violated.	Detail for <i>Path-Profile-Name</i> pane

Table 182: Fields on the Path-Based Steering Profiles Page (*continued*)

Field	Description	Displayed on
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the path-based steering profile.	Detail for <i>Path-Profile-Name</i> pane
Maximum Upstream Burst Size	The maximum upstream burst size (in bytes).	Detail for <i>Path-Profile-Name</i> pane
Maximum Downstream Rate	The maximum downstream rate (in Kbps) for all applications associated with the path-based-steering profile.	Detail for <i>Path-Profile-Name</i> pane
Maximum Downstream Burst Size	The maximum downstream burst size (in bytes).	Detail for <i>Path-Profile-Name</i> pane

RELATED DOCUMENTATION

[Traffic Steering Profiles and SD-WAN Policies Overview](#) | 568

Adding Path-Based Steering Profiles

You can use the Add Path Profile page to add a new path-based steering profile, and specify the traffic type profile, path preference, and advanced configuration for the profile.

To add a path-based steering profile to the tenant:

1. Select **Configuration > SD-WAN > Path-Based Steering Profiles**.

The Path-Based Steering Profiles page appears.

2. Click the add (+) icon.

The Add Path Profile page appears.

3. Enter the path-based steering profile information according to the guidelines provided in [Table 183 on page 603](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the Path-Based Steering Profiles page and a confirmation message indicating that the path-based steering profile was added is displayed. The page refreshes to display the path-based steering profile that you added.

NOTE: After you add a path-based steering profile, you must add an SD-WAN policy intent that references the path-based steering profile in order to enable site-to-site traffic.

Table 183: Fields on the Add Path Profile page

Field	Guidelines
Name	Enter a unique string that can contain alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Traffic Type Profile	Choose a traffic type profile to apply the class-of-service configuration and priority to the SLA profile. You can select a traffic type profile only when it is in the Enabled state.
Path Preference	Select the preferred WAN link type to associate with the SLA profile. The options are MPLS, and Internet.
<i>Advanced Configuration</i>	
Maximum Upstream Rate	Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps
Maximum Upstream Burst Size	Enter the maximum burst size (in bytes). Range: 1 through 1,342,177,280 bytes
Maximum Downstream Rate	Enter the maximum downstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps

Table 183: Fields on the Add Path Profile page *(continued)*

Field	Guidelines
Maximum Downstream Burst Size	Enter the maximum burst size (in bytes). Range: 1 through 1,342,177,280 bytes
Loss Priority	Select a loss priority based on which packets can be dropped or retained when network congestion occurs. The chances of a packet getting dropped is the highest when the loss priority is set to High . Other available values are Medium High , Medium Low , and Low .

RELATED DOCUMENTATION

[Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)
[About the Path-Based Steering Profiles Page | 600](#)
[Editing and Deleting Path-Based Steering Profiles | 604](#)

Editing and Deleting Path-Based Steering Profiles

IN THIS SECTION

- [Editing a Path-Based Steering Profile | 605](#)
- [Deleting a Path-Based Steering Profile | 606](#)

You can use the Path-Based Steering Profiles page to edit and delete path-based steering profiles.

Editing a Path-Based Steering Profile

To edit a path-based steering profile:

NOTE: If you edit a path-based steering profile that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SD-WAN > Path-Based Steering Profiles**.

The Path-Based Steering Profiles page appears.

2. On the Path Profiles tab, select the path-based steering profile that you want to edit.

3. Click the edit (pencil) icon.

The Edit Path Profile page appears displaying the same fields that are presented when you add a path-based steering profile. For more information, see [“Adding Path-Based Steering Profiles” on page 602](#).

4. Modify the fields as needed.

NOTE: You cannot edit the path profile name.

5. Click **OK**.

You are returned to the Path-Based Steering Profiles page. The modifications that you made are saved and a confirmation message is displayed..

Deleting a Path-Based Steering Profile

You can delete path-based steering profiles if they are no longer needed. To delete one or more path-based steering profiles:

NOTE: You cannot delete a path-based steering profile if it is referenced by one or more SD-WAN policy intents.

1. Select **Configuration > SD-WAN > Path-Based Steering Profiles**.

The Path-Based Steering Profiles page appears.

2. On the Path Profiles List tab, select the path profiles that you want to delete.

3. Click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

You are returned to the Path-Based Steering Profiles page. The selected path-based steering profiles are deleted and a confirmation message is displayed.

RELATED DOCUMENTATION

[Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)

[About the Path-Based Steering Profiles Page | 600](#)

[Adding Path-Based Steering Profiles | 602](#)

Breakout and Breakout Profiles Overview

IN THIS SECTION

- [Cloud Breakout | 608](#)
- [Breakout Profiles | 608](#)

- SD-WAN Policy Intents for Breakout | 608
- Benefits of Breakout Profiles | 609

Site-to-site traffic between spoke sites of a tenant is sent (on overlay tunnels) directly from one site to another depending on the tenant topology or through the hub or enterprise hub. However, for Internet-bound or Software as a Service (SaaS) traffic, you can break out the traffic in different ways:

- Local breakout—The traffic exits the VPN directly at the site and goes to the destination.

NOTE: If underlay BGP is enabled for a WAN link, then the routes learnt from BGP are installed for local breakout; CSO does not generate the static default route.

- Backhaul or central breakout—The traffic exits the VPN at the provider hub or at the enterprise hub (if a enterprise hub is associated with the spoke site) and then goes to the destination.
- Cloud breakout—The traffic is sent from the site to a designated cloud-based security platform instead of traffic being sent over an underlay.

NOTE: From CSO Release 4.1.0 onwards, Zscaler is the only cloud-based security platform supported.

In CSO Release 4.0, only local breakout and central breakout (backhaul) are supported and the breakout option is enabled only at the site level. However, from CSO Release 4.1.0 onward, breakout is supported at the site, department, and application (cacheable only) levels by using breakout profiles that are applied using SD-WAN policy intents. Non-cacheable applications follow the site-specific or department-specific behavior as configured in the SD-WAN policy intent.

NOTE: For sites added in CSO Release 4.1.0 onward, you cannot configure breakout *directly* at the site level and must use breakout profiles referenced in SD-WAN policy intents for this purpose.

Cloud Breakout

In releases before CSO Release 5.1.0, as part of providing the tunneled breakout to Zscaler, the tunnel source public IP address was obtained only from the WAN interface. With pool-based NAT supported from Release 5.1.0 onward, the tunnel creation to Zscaler (when pool-based NAT is configured) obtains the source address from the WAN link's NAT pool.

When multiple Zscaler tunnels are needed on a WAN interface (for example, when primary and secondary cloud breakout nodes are configured), the pool IP address must be large enough to accommodate these tunnels. In the case of multiple Zscaler tunnels, no two Zscaler tunnels will have the same source IP address. However, the IP address that is used as Zscaler tunnel's source address, can also be used in the NAT pools.

Breakout Profiles

The following three types of breakout profiles are supported in CSO:

- Local breakout (underlay)
- Backhaul (central breakout)
- Cloud breakout

After you add a breakout profile, you must create an SD-WAN policy intent specifying the source (site, site group, or department) and application and the applicable breakout profile.

SD-WAN Policy Intents for Breakout

For SD-WAN policy intents configured at different source endpoints, the following is applicable:

- Site—A policy intent configured at the site level applies to all the departments within the site. In addition, by default, the site-level configuration is also applicable to all applications because the default configuration for applications is **Any**.
- Department—A policy intent configured at the department level (for tenants with network segmentation enabled) overrides the policy intent configured at the site level. Similar to the behavior for the site-level policy intent, by default, a department-level policy intent is also applicable to all applications because the default configuration for applications is **Any**.
- Application (cacheable only)—A policy intent (at the application level) where you specify one or more cacheable applications overrides the policy intent specified at either the department level or the site level *only* for the specified applications.

Benefits of Breakout Profiles

- Breakout profiles used in intent-based Internet breakout policies (through SD-WAN policy intents) give users granular control over the Internet breakout behavior for specific applications.

RELATED DOCUMENTATION

[Adding Breakout Profiles | 614](#)

[Adding Cloud Breakout Settings | 616](#)

[Creating SD-WAN Policy Intents | 575](#)

About the Breakout Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 610](#)
- [Breakout Profiles Field Descriptions | 610](#)
- [Cloud Breakout Settings Field Descriptions | 612](#)

To access this page, click **Configuration > SD-WAN > Breakout Profiles**.

You can use the Breakout Profiles page to view existing breakout profiles, add local, backhaul, and cloud breakout profiles, edit breakout profiles, and delete breakout profiles. You can also add settings for cloud breakout, edit cloud breakout settings, assign the settings to one or more sites, detach the settings from one or more sites, and delete the settings.

The breakout profiles are displayed on the Breakout Profiles tab and the cloud breakout settings are displayed on the Cloud Breakout Settings tab.

NOTE: Sites with SD-WAN Essentials service do not support cloud breakout profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- View existing breakout profiles—See [Table 184 on page 610](#) for a description of the fields.
- View the details of a breakout profile—On the Breakout Profiles tab, select a breakout profile and from the More menu, select **Detail View**. The Detail for *Breakout-Profile-Name* pane appears on the right-hand side of the page. See [Table 184 on page 610](#) for a description of the fields on this pane.
- View existing cloud breakout settings—(Not applicable to sites with SD-WAN Essentials service.) See [Table 185 on page 612](#) for a description of the fields.
- View the details of cloud breakout settings—(Not applicable to sites with SD-WAN Essentials service.) On the Cloud Breakout Settings tab, select a cloud breakout setting and from the More menu, select **Detail View**. The Detail for *Cloud-Breakout-Setting-Name* pane appears on the right-hand side of the page. See [Table 185 on page 612](#) for a description of the fields on this pane.
- Add a breakout profile—See [“Adding Breakout Profiles” on page 614](#).
- Edit a breakout profile—See [“Editing Breakout Profiles and Cloud Breakout Settings” on page 623](#).
- Delete a breakout profile—See [“Deleting Breakout Profiles and Cloud Breakout Settings” on page 625](#).
- Add cloud breakout settings—See [“Adding Cloud Breakout Settings” on page 616](#).
- Edit cloud breakout settings—See [“Editing Breakout Profiles and Cloud Breakout Settings” on page 623](#).
- Delete cloud breakout settings—See [“Deleting Breakout Profiles and Cloud Breakout Settings” on page 625](#).
- Assign cloud breakout settings to one or more sites—See [“Assigning Cloud Breakout Settings to Sites” on page 620](#).
- Detach cloud breakout settings from one or more sites—See [“Detaching Cloud Breakout Settings from Sites” on page 622](#).

Breakout Profiles Field Descriptions

Table 184: Breakout Profiles Field Descriptions

Field	Description	Displayed On
Name	Name of the breakout profile.	Breakout Profiles page (Breakout Profiles tab) Detail for <i>Breakout-Profile-Name</i> pane
Type	Indicates whether the breakout profile is for local breakout (underlay) or backhaul (central breakout) or cloud breakout.	Breakout Profiles page (Breakout Profiles tab) Detail for <i>Breakout-Profile-Name</i> pane

Table 184: Breakout Profiles Field Descriptions (*continued*)

Field	Description	Displayed On
Description	Description of the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
Path Preference	Indicates the preferred path to be used for breakout traffic: <ul style="list-style-type: none"> • MPLS • Internet • Any, which indicates no preference. 	Breakout Profiles page (Breakout Profiles tab)
Added by	Username of the user who added the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
FqName	Internal name of the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
Rate Limiting	Indicates whether rate limiting is enabled or disabled for the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Downstream Rate	Indicates the maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Downstream Burst Size	Indicates the maximum downstream burst size (in bytes) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Upstream Rate	Indicates the maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Upstream Burst Size	Indicates the maximum upstream burst size (in bytes) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Loss Priority	Indicates the loss priority associated with the breakout profile. The loss priority determines which packets are dropped or retained when network congestion occurs.	Detail for <i>Breakout-Profile-Name</i> pane

Cloud Breakout Settings Field Descriptions

NOTE: Not applicable to sites with SD-WAN Essentials service.

Table 185: Cloud Breakout Settings Field Descriptions

Field	Description	Displayed On
General		
Name or Profile-Name	Name of the cloud breakout setting.	Breakout Profiles page (Cloud Breakout Settings tab) Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Tunnel Type	Overlay tunnel type (IPSEC or GRE) used to break out traffic to the cloud breakout node.	Breakout Profiles page (Cloud Breakout Settings tab) Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Primary Gateway	IPv4 address of the primary cloud breakout node.	Breakout Profiles page (Cloud Breakout Settings tab) Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Primary Link Type	Preferred type of WAN link to be used for breaking out the traffic to the primary cloud breakout node. If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.	Breakout Profiles page (Cloud Breakout Settings tab) Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Secondary Gateway	IPv4 address of the secondary cloud breakout node.	Breakout Profiles page (Cloud Breakout Settings tab) Detail for <i>Cloud-Breakout-Setting-Name</i> pane

Table 185: Cloud Breakout Settings Field Descriptions (*continued*)

Field	Description	Displayed On
Secondary Link Type	Preferred type of WAN link to be used for breaking out the traffic to the secondary cloud breakout node.	Breakout Profiles page (Cloud Breakout Settings tab) Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Sites	If the cloud breakout settings are assigned to one or more sites, the names of the sites are displayed; if not, this field is blank.	Breakout Profiles page (Cloud Breakout Settings tab)
Provider	Name of the cloud service provider.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane
IPSEC Configuration Parameters		
Domain Name	The domain name to generate the fully qualified domain name (FQDN) that is used by the cloud security providers to identify the IPsec tunnel end points. The domain name is populated based on the customer domain name that you provided while onboarding the tenant (Administration Portal > Tenants > Add Tenant > Tenant Properties > Cloud Breakout Settings).	Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Phase 1 Parameters		
Encryption Type	The encryption type for IPsec proposals.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Authentication Type	The IPsec authentication algorithm for security association.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane
DH Group	The Diffie-Hellman (DH) group.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Phase 2 Parameters		
Encryption Type	The encryption type for IPsec proposals.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane

Table 185: Cloud Breakout Settings Field Descriptions (*continued*)

Field	Description	Displayed On
Authentication Type	The IPsec authentication algorithm for security association.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane

RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview](#) | 606

Adding Breakout Profiles

You use the Add Breakout Profile page to add a local breakout (underlay), backhaul, or a cloud breakout profile. A cloud breakout profile is added by Contrail Service Orchestration (CSO) by default.

To add a breakout profile:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, click the add icon (+).

The Add Breakout Profile page appears.

3. Complete the configuration according to the guidelines provided in [Table 186 on page 615](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the Breakout Profiles page (Breakout Profiles tab) and a confirmation message indicating that the breakout profile was added is displayed. The page refreshes to display the breakout profile that you added.

NOTE: After you add a breakout profile, you must add an SD-WAN policy intent that references the breakout profile in order to enable breakout traffic.

Table 186: Fields on the Add Breakout Profile Page

Field	Description
Type	<p>Select the type of breakout profile that you want to add:</p> <ul style="list-style-type: none"> • Local Breakout (Underlay)—Select this option if you want traffic to break out locally (on the underlay) from the site. • Backhaul—Select this option if you want traffic to break out through a hub or a enterprise hub (if configured). • Local Breakout (Cloud)—Select to break out traffic through a cloud-based security platform. Currently, Zscaler is the only cloud-based security platform supported.
Name	Enter a unique name for the breakout profile. You can use alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Description	Enter a description for the breakout profile.
Traffic Type Profile	Select a traffic type profile to apply class of service parameters to the breakout traffic. You can select only a traffic type profile that is enabled.
Preferred Path	<p>Select the preferred path (MPLS, Internet, or Any) to be used for breaking out the traffic.</p> <p>If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.</p> <p>If you specify that any path can be used, then there is no preference and all breakout-enabled links are used in a load-balancing mode.</p>
Advanced Configuration	
Rate Limiting	<p>Click the toggle button to enable rate limiting of breakout traffic for cacheable applications. By default, rate limiting is disabled.</p> <p>If you enable rate limiting, you must specify the upstream and downstream parameters, and the loss priority.</p>
Upstream Rate	Specify the maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
Upstream Burst Size	Specify the maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the upstream rate limit for short periods.
Downstream Rate	Specify the maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.

Table 186: Fields on the Add Breakout Profile Page (*continued*)

Field	Description
Downstream Burst Size	Specify the maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the downstream rate limit for short periods.
Loss Priority	Select a loss priority based on which packets are dropped or retained when network congestion occurs. Packet drops are most likely when the loss priority is High and least likely when the loss priority is Low.

RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 606](#)
[Creating SD-WAN Policy Intents | 575](#)

Adding Cloud Breakout Settings

You use the Add Cloud Breakout Settings page to add cloud breakout settings that you can then apply to sites.

To add cloud breakout settings:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, click the add icon (+).

The Add Cloud Breakout Settings page appears.

3. Complete the configuration according to the guidelines provided in [Table 187 on page 617](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

NOTE: If the gateway is unreachable, an error message **Gateway is unreachable. Do you want to proceed with profile creation?** is displayed. If you want to continue with the cloud breakout profile creation, click **Yes**, else click **Cancel**.

You are returned to the Breakout Profiles page (Cloud Breakout Settings tab) and a confirmation message indicating that the breakout settings are added is displayed.

After you add cloud breakout settings, you can assign the settings to one or more sites. Assigning cloud breakout settings to sites provisions the cloud breakout node (Zscaler) overlay. For traffic to flow, you must reference the cloud breakout profile in an SD-WAN policy intent.

NOTE: Sites with SD-WAN Essentials service do not support cloud breakout profiles.

Table 187: Fields on the Add Cloud Breakout Settings Page

Field	Description
Name	Enter a unique name for the cloud breakout settings. You can use alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Tunnel Type	Select the type of overlay tunnel (IPSEC or GRE) used to break out the traffic to the cloud breakout node.
IPsec Configuration Parameters	
Domain Name	<p>Displays the domain name that is used to generate the fully qualified domain name (FQDN) for SD-WAN policies. The FQDN is used by the cloud security providers to identify the IPsec tunnels. The domain name is populated based on the customer domain name that you provided while onboarding the tenant (Administration Portal > Tenants > Add Tenant > Tenant Properties > Cloud Breakout Settings).</p> <p>Though the domain name is populated automatically, you can modify the domain name.</p>
Phase 1	In Phase 1, the SD-WAN branch site and the cloud breakout node establish a secure tunnel to negotiate the IPsec security associations (SAs).

Table 187: Fields on the Add Cloud Breakout Settings Page (*continued*)

Field	Description
Encryption Type	<p>Select an encryption type for IPsec proposals:</p> <ul style="list-style-type: none"> • AES-256-CBC (default)—Advanced Encryption Standard (AES) 256-bit encryption algorithm in Cipher Block Chaining (CBC) mode. • AES-192-CBC—AES 192-bit encryption algorithm. • AES-128-CBC—AES 128-bit encryption algorithm. • 3DES-CBC—Triple Data Encryption Algorithm (3DES) in CBC mode. Has a block size of 24 bytes; the key size is 192 bits long.
Authentication Type	<p>Select an IPsec authentication algorithm for security association:</p> <ul style="list-style-type: none"> • SHA-256 (default)—Secure Hash Algorithm (SHA) that converts a text of any length into a string of 256 bits. • SHA-384—Produces a 384-bit string. • SHA1—Produces a 160-bit string.
DH Group	<p>Specify the Diffie-Hellman (DH) group to match the IPsec encryption algorithm:</p> <ul style="list-style-type: none"> • GROUP2 (default)—1024-bit Modular Exponential (MODP) algorithm. • GROUP5—1536-bit MODP algorithm. • GROUP14—2048-bit MODP algorithm.
Phase 2	In Phase 2, the SD-WAN spoke site and the cloud breakout node negotiate the IPsec SAs for encrypting and authenticating the exchange of data.
Encryption Type	<p>Select an encryption type for IPsec proposals.</p> <ul style="list-style-type: none"> • NULL (default)—No encryption. This is the default. • AES-256-CBC—AES 256-bit encryption algorithm. • AES-192-CBC—AES 192-bit encryption algorithm. • AES-128-CBC—AES 128-bit encryption algorithm.
Authentication Type	<p>Select an IPsec authentication algorithm for security association.</p> <ul style="list-style-type: none"> • HMAC-MD5-96 (default)—Produces a 128-bit digest. This is the default. • HMAC-SHA-256-128—Produces a 256-bit digest, truncated to 128 bits. • HMAC-SHA1-96—Produces a 160-bit digest.
Protocol	<p>Displays the protocol as ESP (default). Encapsulating Security Payload (ESP) protocol provides a means to ensure privacy (encryption), source authentication and content integrity (authentication).</p> <p>NOTE: You cannot edit the protocol.</p>

Table 187: Fields on the Add Cloud Breakout Settings Page (*continued*)

Field	Description
Primary Gateway	Configuration for the primary cloud breakout node.
Link Type	<p>Select the preferred type of WAN link (MPLS or Internet) to be used for breaking out the traffic to the primary cloud breakout node.</p> <p>If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.</p>
IP Address/Hostname	<p>Enter the IPv4 address or host name of the primary cloud breakout node. Currently, Zscaler is the only cloud-based security platform supported.</p> <p>The IP address or hostname, is validated. If the IP address or host name is not reachable, the Host Unreachable message is displayed.</p>
Preshared Key	<p>Enter the preshared key used for IKE authentication with the primary cloud breakout node. The preshared key is provided by the Zscaler.</p> <p>The key that you enter is masked.</p>
Confirm Preshared Key	Reenter the preshared key for confirmation.
Secondary Gateway	Configuration for the secondary cloud breakout node.
Link Type	<p>Select the preferred type of WAN link (MPLS or Internet) to be used for breaking out the traffic to the secondary cloud breakout node.</p> <p>If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.</p>
IP Address/Hostname	<p>Enter the IPv4 address or host name of the secondary cloud breakout node. Currently, Zscaler is the only cloud-based security platform supported.</p> <p>The IP address or hostname, is validated. If the IP address or host name is not reachable, the Host Unreachable message is displayed.</p>
Preshared Key	<p>Enter the preshared key used for IKE authentication with the secondary cloud breakout node. The preshared key is provided by the Zscaler.</p> <p>The key that you enter is masked.</p>
Confirm Preshared Key	Reenter the preshared key for confirmation.

RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 606](#)[Creating SD-WAN Policy Intents | 575](#)

Assigning Cloud Breakout Settings to Sites

You use the Assign Cloud Breakout Settings to Sites page to assign cloud breakout settings to one or more sites. You assign cloud breakout settings to one or more sites to provision tunnels from the sites to the cloud breakout node. For breakout traffic from the site, the cloud breakout profile must be referenced in an SD-WAN policy intent.

NOTE:

- If you want a site to have cloud breakout enabled, you must assign cloud breakout settings for that site.
- A site can have only one cloud breakout setting associated with it at any given time.
- Sites with SD-WAN Essentials service do not support cloud breakout profiles.

To assign one or more sites to a cloud breakout profile:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, select a cloud breakout profile and click **Assign Sites**.

The Assign Cloud Breakout Settings to Sites page appears displaying the name of the cloud breakout setting and the existing sites to which you can assign the setting. All SD-WAN sites that have local breakout enabled will be displayed in the Available sites column.

3. In the Sites field, select one or more sites in the Available column and click the right arrow icon to move the selected sites to the Selected column. You can also use the search icon on the top right of each column to search for sites names.

Alternatively, if you want to remove sites that you previously selected for assignment, select one or more sites in the Selected column and click the left arrow icon to move the selected sites back to the Available column.

NOTE: You must select at least one site before proceeding.

4. Click **Next**.

The Edit Site Tunnels tab is displayed.

5. Review the configuration and modify the settings, if needed.

- For IPsec Tunnels, ensure that the format for the FQDN is as follows:
 - *Site-name.primary_link.primary_gateway.1@Customer-Domain-Name* for the primary gateway primary link
 - *Site-name.backup_link.primary_gateway.1@Customer-Domain-Name* for the primary gateway backup link
 - *Site-name.primary_link.backup_gateway.1@Customer-Domain-Name* for the secondary gateway primary link
 - *Site-name.backup_link.backup_gateway.1@Customer-Domain-Name* for the secondary gateway backup link

Where *Site-Name* is the name of the site (in CSO) for which the breakout is configured and *Customer-Domain-Name* is the name of the customer domain (in CSO) that you added while onboarding the tenant (**Administration Portal > Tenants > Add Tenant > Tenant Properties > Cloud Breakout Settings**).

- For GRE tunnels, ensure that the primary and secondary gateway internal IP prefix is same as provided by the Zscaler.

6. Select the local links (WAN links) to create the tunnel.

7. Select the link mode as Active-Active or Active-Backup. The primary link is always set to active mode and is used to send the traffic. If secondary link is set to active, the CPE device will load balance the traffic on both primary and secondary links. If the secondary link is set to backup, then secondary link will not be used to send traffic unless the primary link fails.

8. Click **OK**.

A Job is created and you are returned to the Breakout Profiles page (Cloud Breakout Settings tab). After successful completion of the job, the names of the sites to which the settings are assigned are displayed in the Sites column.

RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 606](#)

[Detaching Cloud Breakout Settings from Sites | 622](#)

Detaching Cloud Breakout Settings from Sites

You must detach the cloud breakout settings from one or more sites (by using the Detach Cloud Breakout From Sites page) before editing or deleting the cloud breakout settings.

To detach one or more sites from a cloud breakout profile:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, select a cloud breakout profile and click **Detach Sites**.

The Detach Cloud Breakout From Sites page appears displaying the name of the cloud breakout setting and the existing sites to which the setting was assigned.

3. In the **Sites** field, select one or more sites in the Available column and click the right arrow icon to move the selected sites to the Selected column. You can also use the search icon on the top right of each column to search for sites.

Alternatively, if you want to remove the selected sites, select one or more sites in the Selected column and click the left arrow icon to move the selected sites back to the Available column.

NOTE: You must select at least one site before proceeding to the next step.

4. Click **Save**.

A job is created and you are returned to the Breakout Profiles page (Cloud Breakout Settings tab). After successful completion of the job, the names of the sites to which the settings are detached are removed from the Sites column of the cloud breakout settings tab.

RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 606](#)

[Assigning Cloud Breakout Settings to Sites | 620](#)

Editing Breakout Profiles and Cloud Breakout Settings

IN THIS SECTION

- [Editing Breakout Profiles | 623](#)
- [Editing Cloud Breakout Settings | 624](#)

On the Breakout Profiles page, you can edit breakout profiles and cloud breakout settings that are not assigned to sites.

NOTE: You cannot edit the cloud breakout profile that is automatically created by Contrail Service Orchestration (CSO). Also, sites with SD-WAN Essentials service do not support cloud breakout profiles.

Editing Breakout Profiles

To edit a breakout profile:

NOTE: If you edit a breakout policy that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, select the breakout profile that you want to edit.

3. Click the edit (pencil) icon.

The Edit Breakout Profile page appears displaying the same fields that are presented when you add a breakout profile. For more information, see [“Adding Breakout Profiles” on page 614](#).

4. Modify the fields as needed.

NOTE: You can modify only some fields when you are editing a breakout profile

5. Click **OK**.

You are returned to the Breakout Profiles page. The modifications that you made are saved and a confirmation message is displayed.

Editing Cloud Breakout Settings

Before editing a cloud breakout setting, ensure that the setting is detached from the site. The edit (pencil) icon is disabled for cloud breakout settings that are assigned to sites.

To edit cloud breakout settings that are not assigned to sites:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, select the cloud breakout setting that you want to edit.

3. Click the edit (pencil) icon.

The Edit Cloud Breakout page appears displaying the same fields that are presented when you add cloud breakout settings. For more information, see [“Adding Cloud Breakout Settings” on page 616](#).

4. Modify the fields as needed.

NOTE: You can modify only some fields when you are editing a breakout profile

5. Click **OK**.

You are returned to the Breakout Profiles page. The modifications that you made are saved and a confirmation message is displayed.

RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 606](#)

[About the Breakout Profiles Page | 609](#)

Deleting Breakout Profiles and Cloud Breakout Settings

IN THIS SECTION

- [Deleting Breakout Profiles | 625](#)
- [Deleting Cloud Breakout Settings | 625](#)

On the Breakout Profiles page, you can delete breakout profiles that are not used in SD-WAN policy intents and cloud breakout settings that are not assigned to sites.

Deleting Breakout Profiles

To delete a breakout profile that is not used in an SD-WAN policy intent:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, select the breakout profile that you want to delete.

3. Click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

You are returned to the Breakout Profiles page. The selected breakout profile is deleted and a confirmation message is displayed.

Deleting Cloud Breakout Settings

Before deleting a cloud breakout setting, ensure that the setting is detached from the site. The delete (trash can) icon is disabled for cloud breakout settings that are assigned to sites.

To delete cloud breakout settings that are not assigned to sites:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, select the cloud breakout setting that you want to delete.

3. Click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

You are returned to the Breakout Profiles page. The selected cloud breakout setting is deleted and a confirmation message is displayed.

RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 606](#)

[About the Breakout Profiles Page | 609](#)

[Detaching Cloud Breakout Settings from Sites | 622](#)

Configuring Breakout on SD-WAN Sites

The following is the workflow for configuring breakout (local breakout [underlay], backhaul [central breakout], or cloud breakout):

1. *Before* configuring breakout, ensure that you complete the following tasks:
 - a. If you are using enterprise hub sites, add, configure, and activate one or more enterprise hub sites. See [“Add Enterprise Hubs with SD-WAN Capability” on page 76](#).
 - b. Add, configure, and activate one or more branch sites with SD-WAN capability. See [“Add a Branch Site with SD-WAN Capability” on page 120](#).

NOTE: You must attach a branch site with SDWAN capability to a provider hub site or an enterprise hub site, or to both hub sites.

- c. (Optional) If you are using application-based breakout, ensure that you install the application ID license (if it is required for the device) and signatures on the devices (associated with the sites).
2. Depending on the type of breakout you are configuring, add one or more breakout profiles for the following types of breakout:
 - Local breakout (underlay)
 - Backhaul (central breakout)
 - Cloud breakout

See [“Adding Breakout Profiles” on page 614](#).
 3. For cloud breakout, add cloud breakout settings and then assign the cloud breakout settings to one or more branch or enterprise hub sites. See [“Adding Cloud Breakout Settings” on page 616](#) and [“Assigning Cloud Breakout Settings to Sites” on page 620](#).
 4. Add one or more SD-WAN policy intents in which you reference the previously-added breakout profiles. See [“Creating SD-WAN Policy Intents” on page 575](#).
 5. Deploy the SD-WAN policy. See [“Deploying Policies” on page 742](#).
 6. Configure firewall policy intents to allow Internet-bound traffic from the sites or departments for which you configured breakout (through the SD-WAN policy intent). See [“Adding Firewall Policy Intents” on page 449](#).
 7. Deploy the firewall policy. See [“Deploying Policies” on page 742](#).
 8. For cloud breakout using Zscaler, ensure that the user IDs in the Zscaler account are configured as follows:
 - *Site-Name.primary.1@Tenant-Name.com* for the primary tunnel
 - *Site-Name.backup.1@Tenant-Name.com* for the secondary tunnel

Where *Site-Name* is the name of the site (in CSO) for which the breakout is configured and *Tenant-Name* is the name of the tenant (in CSO) to which the site belongs.

RELATED DOCUMENTATION

| [Breakout and Breakout Profiles Overview](#) | 606

Managing NAT Policies

IN THIS CHAPTER

- [NAT Policies Overview | 629](#)
- [About the NAT Policies Page | 632](#)
- [Creating NAT Policies | 633](#)
- [Editing and Deleting NAT Policies | 635](#)
- [About the Single NAT Policy Page | 636](#)
- [Creating NAT Policy Rules | 638](#)
- [Editing, Cloning, and Deleting NAT Policy Rules | 645](#)
- [Deploying NAT Policy Rules | 647](#)
- [Selecting NAT Source | 648](#)
- [Selecting NAT Destination | 652](#)
- [NAT Pools Overview | 656](#)
- [About the NAT Pools Page | 656](#)
- [Creating NAT Pools | 658](#)
- [Editing, Cloning, and Deleting NAT Pools | 660](#)
- [Deploying NAT Policies | 662](#)
- [Importing NAT Policies | 662](#)

NAT Policies Overview

Network Address Translation (NAT) is a form of network masquerading where you can hide devices or sites between zones or interfaces. A trusted zone is a segment of a network on which security measures are applied. It is usually assigned to the internal LAN. An example of an untrusted zone is the internet. NAT modifies the IP addresses of the packets moving between the trusted and untrusted zones.

Whenever a packet exits a NAT device (when traversing from the internal LAN to the external WAN), the device performs a translation on the packet's IP address by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This process hides your internal IP addresses from the other networks and keeps your network secure.

Using NAT also enables you to use more internal IP addresses. As these IP addresses are hidden, there is no risk of conflict with an IP address from a different network. This helps you conserve IP addresses.

CSO supports three types of NAT:

- **Source NAT**— Translates the source IP address of a packet leaving a trust zone (outbound traffic). It translates the traffic originating from the device in the trust zone. The source IP address of the traffic (which is a private IP address), is translated to a public IP address that can be accessed by the destination device specified in the NAT rule. The destination IP address is not translated.

The following uses cases show the support for source NAT translation between IPv6 and IPv4 address domains:

- Translation from one IPv6 subnet to another IPv6 subnet without Network Address Port Translation (NAPT), also known as Port Address Translation (PAT).
- Translation from IPv4 addresses to IPv6 prefixes along with IPv4 address translation.
- Translation from IPv6 hosts to IPv6 hosts with or without NAPT.
- Translation from IPv6 hosts to IPv4 hosts with or without NAPT.
- Translation from IPv4 hosts to IPv6 hosts with or without NAPT.
- **Destination NAT**—Translates the destination IP address of a packet. Using destination NAT, an external device can send packets to a hidden internal device. As an example, consider the case of a webserver behind a NAT device. Traffic to the WAN-facing public IP address (the destination IP address) is translated to the internal webserver private IP address.

The following uses cases show the support for destination NAT translation between IPv6 and IPv4 address domains:

- Mapping of one IPv6 subnet to another IPv6 subnet
- Mapping between one IPv6 host and another IPv6 host

- Mapping of one IPv6 host (and optional port number) to another special IPv6 host (and optional port number)
- Mapping of one IPv6 host (and optional port number) to another special IPv4 host (and optional port number)
- Mapping of one IPv4 host (and optional port number) to another special IPv6 host (and optional port number)
- Static NAT— Always translates a private IP address to the same public IP address. It translates traffic from both sides of the network (both source and destination). For example, a web-server with a private IP address can access the Internet using a static, one-to-one address translation. In this case, outgoing traffic from the web-server undergoes source NAT translation, and incoming traffic to the web-server undergoes destination NAT translation.

The following uses cases show the support for static NAT translation between IPv6 and IPv4 address domains:

- Mapping of one IPv6 subnet to another IPv6 subnet.
- Mapping between one IPv6 host and another IPv6 host.
- Mapping between IPv4 address *a.b.c.d* and IPv6 address *Prefix::a.b.c.d*.
- Mapping between IPv4 hosts and IPv6 hosts.
- Mapping between IPv6 hosts and IPv4 hosts.

CSO also supports persistent NAT where address translations are maintained in the database for a configurable amount of time after a session ends.

[Table 188 on page 630](#) shows the persistent NAT support for different source NAT and destination NAT addresses.

Table 188: Persistent NAT Support

Source NAT Address	Translated Address	Destination NAT Address	Persistent NAT
IPv4	IPv6	IPv4	No
IPv4	IPv6	IPv6	No
IPv6	IPv4	IPv4	Yes
IPv6	IPv6	IPv6	No

[Table 189 on page 631](#) and [Table 190 on page 631](#) show the translated address pool selection for source NAT, destination NAT, and static NAT addresses.

Table 189: Translated Address Pool Selection for Source NAT

Source NAT Address	Destination Address	Pool Address
IPv4	IPv4	IPv4
IPv4	IPv6 - Subnet must be greater than 96	IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv6

Table 190: Translated Address Pool Selection for Destination NAT And Static NAT

Source NAT Address	Destination Address	Pool Address
IPv4	IPv4	IPv4 or IPv6
IPv4	IPv6 - Subnet must be greater than 96	IPv4 or IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv4 or IPv6

NOTE:

- For source NAT, the proxy Neighbor Discovery Protocol (NDP) is available for NAT pool addresses. For destination NAT and static NAT, the proxy NDP is available for destination NAT addresses.
- A NAT pool can have a single IPv6 subnet or multiple IPv6 hosts.
- You cannot configure the overflow pool if the address type is IPv6.
- NAT pools permit address entries of only one version type: IPv4 or IPv6.

RELATED DOCUMENTATION
[About the NAT Policies Page | 632](#)
[Creating NAT Policies | 633](#)
[Editing and Deleting NAT Policies | 635](#)
[Editing, Cloning, and Deleting NAT Policy Rules | 645](#)

About the NAT Policies Page

To access this page, select **Configuration > NAT > NAT Policies**.

Use the **NAT Policies** page to create, modify, clone, and delete NAT policies and policy rules. You can filter and sort this information to get a better understanding of what you want to configure.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT policy. See [“Creating NAT Policies” on page 633](#).
- Modify or delete a NAT policy. See [“Editing and Deleting NAT Policies” on page 635](#).
- Create, modify, clone, and delete NAT policy rules. See [“About the Single NAT Policy Page” on page 636](#).
- Search for a specific NAT policy. Click the Search icon in the top right corner of the page to search for a NAT policy.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

Field Descriptions

[Table 191 on page 632](#) provides guidelines on using the fields on the **NAT Policies** page.

Table 191: Fields on the NAT Policies Page

Field	Description
Name	Displays the name of the NAT policy.
Installed On	Displays the sites on which the NAT policy is assigned.
Rules	Number of rules assigned to the NAT policy.
Undeployed	Number of undeployed rules associated with the NAT policy.

RELATED DOCUMENTATION

[NAT Policies Overview | 629](#)

Creating NAT Policies | 633

Editing and Deleting NAT Policies | 635

About the Single NAT Policy Page | 636

Creating NAT Policies

Use the Create NAT Policy page to create NAT policies.

To create a NAT policy:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Click the add icon (+).

The **Create NAT Policy** page displays fields required for creating and configuring a NAT policy.

3. Complete the configuration according to the guidelines provided in [Table 192 on page 633](#).

NOTE: You can associate only a single device or a device cluster with a site.

4. Click **OK** to save the changes.

A NAT policy with the configuration you provided is created.

Table 192: Fields on the Create NAT Policy Page

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.
Description	Enter a description for the policy; the maximum length is 1024 characters.

Table 192: Fields on the Create NAT Policy Page (*continued*)

Field	Description
Manage Auto-Proxy ARP	<p>The Address Resolution Protocol (ARP) protocol translates IPv4 addresses to MAC addresses. Typically, an interface responds with its MAC address only when an ARP request for its IP address is received.</p> <p>A proxy ARP implies that the same interface will proxy for other IP addresses (that is, respond to ARP requests for other IP addresses).</p> <p>Managing a proxy ARP automatically enables the selection of an appropriate interface for any address (as part of a NAT rule) that is not an actual interface address. Proxy ARP management applies to translated addresses in a source NAT rule or to a destination address in a destination NAT rule.</p> <p>NOTE: When creating a source NAT rule with pool translation, the address pool assigned must be in the same subnet as the outgoing interface selected.</p> <p>NOTE: When creating a destination NAT rule, the external WAN interface can be a proxy for another IP address in the same subnet as the original IP address of the interface.</p>
Sites Applied On	<p>Select the sites on which you want to apply the policy in the Available column and move them to the Selected column by clicking the greater-than icon (>).</p> <p>NOTE: The Available column lists only those sites that do not have a NAT policy associated with them.</p>
Sequence No.	<p>Click Select Policy Sequence. The Select Policy Sequence page appears, displaying all NAT policies. Select the policy you want to reorder and select Move Policy Up or Move Policy Down to reorder your NAT policy among the existing policies.</p>

RELATED DOCUMENTATION

[NAT Policies Overview | 629](#)
[About the NAT Policies Page | 632](#)
[Editing and Deleting NAT Policies | 635](#)
[About the Single NAT Policy Page | 636](#)
[Creating NAT Policy Rules | 638](#)
[Editing, Cloning, and Deleting NAT Policy Rules | 645](#)

Editing and Deleting NAT Policies

IN THIS SECTION

- [Editing NAT Policies | 635](#)
- [Deleting NAT Policies | 635](#)

You can edit or delete a NAT policy from the **NAT Policies** page.

Editing NAT Policies

To modify the parameters configured for a NAT Policy:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Hover over the NAT policy you want to edit, and then click on the edit icon (pencil symbol) on the right side of the table.

The **Edit NAT Policy** page appears, showing the same fields as those seen when you create a new NAT policy.

3. Modify the parameters according to the guidelines provided in [“Creating NAT Policies” on page 633](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, you will see the modified NAT policy in the **NAT Policies** page.

Deleting NAT Policies

To delete a NAT policy:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Hover over the NAT policy you want to delete and then click the delete icon (X).

An alert message appears, verifying that you want to delete your selection.

3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the NAT policy is deleted.

NOTE: When the NAT policy is deleted, the NAT rules associated with the policy are deleted from device.

RELATED DOCUMENTATION

[NAT Policies Overview | 629](#)

[About the NAT Policies Page | 632](#)

[Creating NAT Policies | 633](#)

[Editing, Cloning, and Deleting NAT Policy Rules | 645](#)

About the Single NAT Policy Page

To access this page, select **Configuration > NAT > NAT Policies**. The **NAT Policies** page appears displaying all existing NAT policies. Click on a NAT policy to view the rules associated with it.

The *Single NAT Policy* page displays the NAT rules associated with the NAT policy, and keep track of the number and order of rules for each policy. You can also create a new NAT rule, modify the configured parameters of existing NAT rules, clone, and delete NAT rules, using this page.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT rule. See [“Creating NAT Policy Rules” on page 638](#).
- Update the sequence of the NAT rules using the up and down arrows that appear when you hover over the NAT rule.
- Modify, clone, and delete NAT rules. See [“Editing, Cloning, and Deleting NAT Policy Rules” on page 645](#).
- Deploy a NAT rule. See [“Deploying NAT Policy Rules” on page 647](#).
- Search for a specific NAT rule. Click the Search icon in the top right corner of the page to search for a NAT rule.
- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

Field Descriptions

Table 193 on page 637 provides information on the fields in the NAT rules contained within this NAT policy.

Table 193: Fields on the Single NAT Policy Page

Field	Description
Source	Displays the source endpoint on which the NAT policy applies. A source endpoint can be an address, protocol, interface, routing instance, zone, or port.
Destination	Displays the destination endpoint on which the NAT policy applies. A destination endpoint can be an address, interface, service, routing instance, zone, or port.
Translation	Displays the translation type applied on the incoming or outgoing traffic.
Details	Displays the type of NAT rule. A NAT rule can be of type source, static, or destination.

The **Total Rules** field on the top right corner of the page displays the total number of rules associated with the NAT policy. The **Undeployed** field displays the number of undeployed rules associated with the NAT policy. To deploy undeployed rules, click **Deploy**. See “[Deploying NAT Policy Rules](#)” on page 647.

RELATED DOCUMENTATION

NAT Policies Overview	 629
About the NAT Policies Page	 632
Creating NAT Policies	 633
Editing and Deleting NAT Policies	 635
Creating NAT Policy Rules	 638
Editing, Cloning, and Deleting NAT Policy Rules	 645
Deploying NAT Policy Rules	 647

Creating NAT Policy Rules

NAT processing centers on the evaluation of NAT rule sets and rules. A rule set determines the overall direction of the traffic to be processed. After a rule set that matches the traffic is found, each rule in the rule set is evaluated for a match. NAT rules can match on the following packet information:

- Source and destination address
- Source port (for source and static NAT only)
- Destination port

The first rule in the rule set that matches the traffic is used. If a packet matches a rule in a rule set during session establishment, traffic is processed according to the action specified by that rule.

To create a new NAT rule, click the NAT policy name. The *Single NAT Policy* page appears, providing you with options to configure NAT rules. Alternately, you can click on the rule number listed under **Rules** against the policy, to create a new rule. You can configure the following types of NAT rules:

- **Static**—To add a static NAT rule, click **Add Static NAT Rule** or click **Create** on the top right corner and select **Static**.
- **Source**—To add a source NAT rule, click **Add Source NAT Rule** or click **Create** on the top right corner and select **Source**.
- **Destination**—To add a destination NAT rule, click **Add Destination NAT Rule** or click **Create** on the top right corner and select **Destination**.

Depending on the type of rule you have chosen, some fields in the rule will not be applicable. In addition to defining rules between zones and interfaces, you can define NAT rules with virtual routers defined on the device. These rules can be successfully published and updated on the device.

To create a NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the existing NAT policies.

2. Click the name of the NAT policy for which you want to create rules. Alternately, you can click on the number listed under **Rules** against a NAT policy.

The *Single NAT Policy* page appears.

3. Click **Create** and select either **Source**, **Static**, or **Destination**. The page displays fields for creating a NAT rule.

4. Complete the configuration according to the guidelines provided in [Table 194 on page 639](#).
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A NAT rule with the configuration you provided is created.

[Table 194 on page 639](#) provides guidelines on using the fields on the **Single NAT Policy** page.

Table 194: Fields on the Single NAT Policy Page for Creating NAT Rules

Field	Description
Source	<p>Click the add icon (+) to select the source endpoints on which the NAT policy rule applies, from the displayed list of addresses, protocols, interfaces, routing instances, zones, or ports.</p> <p>The possible endpoints for source differ based on whether the NAT rule is a source, destination, or static NAT rule.</p> <ul style="list-style-type: none"> • The possible endpoints for source for a source NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Protocols • Ports • VRF Groups • The possible endpoints for source for a destination NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Protocols • VRF Groups • The possible endpoints for source for a static NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Ports • VRF Groups <p>You can also select a source endpoint by using the methods described in “Selecting NAT Source” on page 648.</p>

Table 194: Fields on the Single NAT Policy Page for Creating NAT Rules (*continued*)

Field	Description
Destination	<p>Click the add icon (+) to select the destination endpoints on which the NAT policy rule applies, from the displayed list of addresses, interfaces, services, routing instances, zones, or ports.</p> <p>The possible endpoints for destination differ based on whether the NAT rule is a source, destination, or static NAT rule.</p> <ul style="list-style-type: none"> • The possible endpoints for destination for a source NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Services • Ports • VRF Groups • The possible endpoints for destination for a destination NAT rule are: <ul style="list-style-type: none"> • Addresses • Services • Ports • The possible endpoints for destination for a static NAT rule are: <ul style="list-style-type: none"> • Addresses • Ports <p>You can select a destination endpoint by using the methods described in “Selecting NAT Destination” on page 652.</p> <p>NOTE: When you create a destination NAT rule for traffic arriving on an interface that terminates a VPN link, the translation process may break the VPN link. This will happen if the destination address in a destination NAT rule is specified only as the WAN-facing IP address of that interface. For example, in the following NAT rule, any traffic destined to Wan.IP will get translated to the destination pool and will break functionality of the VPN link packets terminating on this interface.</p> <p>[Any.Address] --> [Wan.IP] :: [Dest-Pool-1]</p> <p>Therefore, the recommendation in such cases is to use a destination NAT rule with destination field as [Address + Port]. For example:</p> <p>[Any.Address] --> [Wan.IP + Port] :: [Dest-Pool-1]</p>
Translation	

Table 194: Fields on the Single NAT Policy Page for Creating NAT Rules (*continued*)

Field	Description
Translation Type	<p>Specify the translation type for the incoming traffic. The translation options vary based on whether you are creating a source, static, or destination NAT rule.</p> <p>Chose one among the following translation types for a source NAT rule:</p> <ul style="list-style-type: none"> • None—No translation is required for the incoming traffic. • Interface—Performs interface-based translations on the source or destination packet. • Pool—Performs pool-based translations on the source or destination packet. Click on the add icon (+) in the Select Pool field to choose the translation pool. <p>You can also create a new pool by clicking Add new pool. See “Creating NAT Pools” on page 658.</p> <p>Chose one among the following translation types for a static NAT rule:</p> <ul style="list-style-type: none"> • Address—Performs address-based translations on the source or destination packet. Click on the add icon (+) in the Select Address field to choose the translation address. <p>You can also create a new address by clicking Add new address. See “Creating Addresses or Address Groups” on page 753.</p> <p>NOTE: In an SD-WAN environment, it is mandatory that you select the routing instance corresponding to the translation address. You can select the routing instance for a translation address using the Advanced Settings page. For more information on Advanced Settings, see Table 196 on page 644.</p> <ul style="list-style-type: none"> • Corresponding IPv4—Uses the corresponding IPv4 address to perform translations on the source or destination packet. <p>Chose one among the following translation types for a destination NAT rule:</p> <ul style="list-style-type: none"> • None—No translation is required for the incoming traffic. • Pool—Performs pool-based translations on the source or destination packet. Click on the add icon (+) in the Select Pool field to choose the translation pool. <p>You can also create a new pool by clicking Add new pool. See “Creating NAT Pools” on page 658.</p> <p>NOTE: In an SD-WAN environment, the destination NAT pool selected should be configured with a site and a routing instance corresponding to the pool address. For example, a webserver with IP address (IP1) is running in the HR department. To create a destination NAT pool corresponding to this webserver IP address, you must specify the following mandatory fields while creating the NAT pool:</p> <p>Address - IP1</p> <p>Site - the site hosting the webserver</p> <p>Routing instance - natVR_HR</p>

Table 194: Fields on the Single NAT Policy Page for Creating NAT Rules (*continued*)

Field	Description
Advanced Settings (Optional)	Click Configure to configure advance settings for a source or static NAT rule. For more information about advanced settings for the translation types Interface and Pool for a source NAT rule, see Table 195 on page 642 . For more information about advanced settings for the translation types Interface and Pool for a static NAT rule, see Table 196 on page 644
Details	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.
Description	Enter a description for the policy intent; maximum length is 1024 characters.
End Points	<p>Create source and destination endpoints such as addresses and services.</p> <ul style="list-style-type: none"> • To create an address, click the add icon (+) and select Address. See “Creating Addresses or Address Groups” on page 753 to configure the parameters of the address. • To create a service, click the add icon (+) and select Service. See “Creating Services and Service Groups” on page 759 to configure the parameters of the service. <p>To edit the configured parameters of an address or service, hover over it and click on the edit icon (pencil symbol).</p>

[Table 195 on page 642](#) provides guidelines on using the fields on the **Advanced Settings** page for a source NAT rule.

Table 195: Fields on the Advanced Settings Page for Source NAT Rule

Field	Description
Persistent	<p>Enable the check box to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address.</p> <p>NOTE: For persistence to be applicable for the NAT policy, ensure that port overloading is turned off for the device to which the NAT policy is applicable. Use the following command to turn off port overloading for a device:</p> <pre>[Edit mode] set security nat source interface port-overloading off</pre>

Table 195: Fields on the Advanced Settings Page for Source NAT Rule (*continued*)

Field	Description
Persistent NAT Type	<p>Configure persistent NAT mappings.</p> <ul style="list-style-type: none"> • Permit any remote host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. (The reflexive transport address is the public IP address and port created by the NAT device closest to the STUN server.) Any external host can send a packet to the internal host by sending the packet to the reflexive transport address. • Permit target host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address. • Permit target host port—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address and port.
Inactivity Timeout	<p>The amount of time, in seconds, that the persistent NAT binding remains in the site's memory when all the sessions of the binding entry have ended. When the configured timeout is reached, the binding is removed from memory. The value of the inactivity timeout can range from 60 through 7200 seconds. The default value of the inactivity timeout is 60 seconds.</p>
Maximum Session Number	<p>Maximum session number—The maximum number of sessions with which a persistent NAT binding can be associated. For example, if the maximum session number of the persistent NAT rule is 65,536, then a 65,537th session cannot be established if that session uses the persistent NAT binding created from the persistent NAT rule.</p> <p>The range is 8 through 65,536. The default is 30 sessions.</p>
Address Mapping	Select an address from the available list.
Pool Address	Displays the NAT pool address.
Host Address Base	Displays the base address of the original source IP address range. The host address base is used for IP address shifting.
Port Translation	Displays whether port translation is enabled or disabled for this NAT rule.
Overflow Pool Type	Displays the source pool to be used when the current address pool is exhausted.
Overflow Pool Name	Displays the name of the overflow pool.

Table 195: Fields on the Advanced Settings Page for Source NAT Rule (*continued*)

Field	Description
Mapped Port Type	<p>Specify the type of port mapping:</p> <ul style="list-style-type: none"> • Port—Enter a value for Port, ranging from 0 through 65,535. • Range—Enter the port range values in the Start and End fields, ranging from 0 through 65,535.

[Table 196 on page 644](#) provides guidelines on using the fields on the **Advanced Settings** page for a static NAT rule.

Table 196: Fields on the Advanced Settings Page for Static NAT Rule

Field	Description
Mapped Port Type	<p>Specify the type of port mapping:</p> <ul style="list-style-type: none"> • Port—Enter a value for Port, ranging from 0 through 65,535. • Range—Enter the port range values in the Start and End fields, ranging from 0 through 65,535.
Routing Instance	Select the routing instance for the static NAT rule.

RELATED DOCUMENTATION

[About the Single NAT Policy Page | 636](#)

[Editing, Cloning, and Deleting NAT Policy Rules | 645](#)

[Deploying NAT Policy Rules | 647](#)

[NAT Policies Overview | 629](#)

[About the NAT Policies Page | 632](#)

[Creating NAT Policies | 633](#)

[Editing and Deleting NAT Policies | 635](#)

Editing, Cloning, and Deleting NAT Policy Rules

IN THIS SECTION

- [Editing NAT Policy Rules | 645](#)
- [Cloning NAT Policy Rules | 645](#)
- [Deleting NAT Policy Rules | 646](#)

You can edit, clone, or delete a NAT policy rule from the **NAT Policy** page.

Editing NAT Policy Rules

To modify the parameters configured for an NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Select the NAT policy whose rules you want to edit.

The selected **NAT Policy** appears, displaying the rules associated with the NAT policy.

3. Hover over the NAT policy rule that you want to modify and click on the edit icon (pencil symbol) that appears on the right side of the NAT policy rule. The page changes to display the same fields that you use to create a NAT policy rule.

4. Complete the configuration according to the guidelines provided in [“Creating NAT Policy Rules” on page 638](#).

5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified NAT policy rule appears on the **NAT Policy** page.

Cloning NAT Policy Rules

To clone a NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Select the NAT policy whose rule you want to clone.

The selected **NAT Policy** appears, displaying the rules associated with the NAT policy.

3. Hover over the NAT policy rule that you want to clone and click on the clone icon that appears on the right side of the NAT policy rule.

The cloned NAT policy rule appears below the current rule.

You can modify the parameters configured for the cloned NAT policy rule or rename it as required.

Deleting NAT Policy Rules

To delete a NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Select the NAT policy whose rule you want to delete.

The selected **NAT Policy** appears, displaying the rules associated with the NAT policy.

3. Hover over the NAT policy rule you want to delete and then click the delete icon **(X)**.

An alert message appears, verifying that you want to delete your selection.

4. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected NAT policy rule is deleted.

RELATED DOCUMENTATION

[About the Single NAT Policy Page | 636](#)

[Creating NAT Policy Rules | 638](#)

[Deploying NAT Policy Rules | 647](#)

[NAT Policies Overview | 629](#)

[About the NAT Policies Page | 632](#)

[Creating NAT Policies | 633](#)

[Editing and Deleting NAT Policies | 635](#)

Deploying NAT Policy Rules

To deploy an NAT policy rule:

1. Select **Configuration > NAT Policy > Policies**.

2. Click on the name of the NAT policy rules displayed.

The NAT policy rule page appears.

3. Click **Deploy**.

The **Deploy** page appears.

4. Configure your deployment as required. See [“Deploying Policies” on page 742](#).

All the NAT policy rules associated with the NAT policy are deployed. That is, the entire NAT policy is deployed.

NOTE: By default, all the NAT policy rules associated with the NAT policy (the entire NAT policy) are deployed when you click **Deploy**. Suppose you select a particular NAT policy rule and click **Deploy**, even then, all the NAT policy rules associated with that NAT policy are deployed.

RELATED DOCUMENTATION

[About the Single NAT Policy Page | 636](#)

[Creating NAT Policy Rules | 638](#)

[Editing, Cloning, and Deleting NAT Policy Rules | 645](#)

[NAT Policies Overview | 629](#)

[About the NAT Policies Page | 632](#)

[Creating NAT Policies | 633](#)

[Editing and Deleting NAT Policies | 635](#)

Selecting NAT Source

IN THIS SECTION

- [Adding an Endpoint as NAT Source | 648](#)
- [Selecting Interfaces when GWR Resides Inside an NFX Box | 648](#)
- [Selecting NAT Source Using Abbreviations | 649](#)
- [Selecting a NAT Source from the End Points Panel | 650](#)
- [Creating and Selecting a NAT Source from the End Points Panel | 650](#)
- [Creating Addresses from Source Field | 651](#)

The following procedures provides various methods using which you can choose an endpoint as a NAT source:

Adding an Endpoint as NAT Source

View and select the source endpoint from the complete list of addresses, protocols, interfaces, zones, routing instances, or ports.

1. Click the **Source** field. A list of relevant endpoints are displayed.
2. Click the **View more results** link provided at the bottom of the source endpoints. The complete list of addresses, protocols, interfaces, and ports is displayed in the **End Points** panel on the right.
3. (Optional) Click the edit icon to edit the address, protocol, interface, zones, routing instances, or port endpoint.
4. Click check mark icon (✓) to select the endpoint as a source.

Selecting Interfaces when GWR Resides Inside an NFX Box

The physical interfaces of an NFX box are mapped to the virtual interfaces of the Gateway Router (GWR) (vSRX) as given in [Table 197 on page 649](#). These are the default mappings provided by CSO. You may change these interface mappings based on your requirements.

Table 197: NFX and GWR Interface Mapping

NFX Physical Interface	GWR Virtual Interface
WAN 0 (ge-0/0/10)	ge-0/0/2
WAN 1 (ge-0/0/11)	ge-0/0/3
WAN 2 (xe-0/0/12)	ge-0/0/7
WAN 3 (xe-0/0/13)	ge-0/0/8
LAN-X (ge-0/0/X)	Ge-0/0/06.<vlan-id-for-X>

When you create a new NAT rule and an NFX physical interface is intended as the source endpoint, select the respective mapped GWR interface.

Selecting NAT Source Using Abbreviations

Enter an abbreviation in the **Source** field to select the source endpoint from a filtered list of source endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of protocols, enter **PROT** or **prot**.
- To view a filtered list of interfaces, enter **INTR** or **intr**.
- To view a filtered list of zones, enter **ZONE** or **zone**.
- To view a filtered list of routing instances, enter **ROUT** or **rout**.

Click the endpoints in the filtered list to select them.

You can add a port number as a source endpoint. To do so:

1. Type **PORT** or **port** in the **Source** field.
2. Press Tab.
3. Enter the port number and press Enter.

You can also enter a range of ports by using the separator -. For example, you can enter **10-20**.

The entered port value is selected as a source endpoint.

You can also select the endpoint from the complete list of addresses, protocols, interfaces, zones, and routing instances. See [“Adding an Endpoint as NAT Source” on page 648](#).

Selecting a NAT Source from the End Points Panel

You can select a NAT source endpoint from the **End Points** panel. Alternately, you can create a new NAT source endpoint from the **End Points** panel, see [“Creating and Selecting a NAT Source from the End Points Panel” on page 650](#).

To select an NAT source endpoint from the **End Points** panel:

1. Click the **Source** field.

2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, interfaces, protocols, zones, and routing instances.

3. (Optional) To view more information about a source endpoint, click the details icon on the right of the endpoint. To edit the source endpoint, click the edit icon (pencil symbol) on the right of the endpoint.

NOTE: You can only edit or view details of a source endpoint if these options appear on right side of the endpoint when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the endpoint as a source.

Creating and Selecting a NAT Source from the End Points Panel

To create a new source endpoint from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of endpoint you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to create a new endpoint.

- To create a new address, see [“Creating Addresses or Address Groups” on page 753](#).
- To create a new service, see [“Creating Services and Service Groups” on page 759](#).
- To create a new NAT pool, see [“Creating NAT Pools” on page 658](#).

After the endpoint is created, it appears in the **Endpoints** panel.

2. Click the check mark icon (✓) to add the new endpoint as a source.

Creating Addresses from Source Field

You can use one of the following ways to create a new address from the **Source** field and use the newly created address as a source endpoint:

- Type the address directly in the **Source** field. If the address is valid, it is created immediately and added as a source endpoint.
- Create an address from the **Source** field, using the following steps:
 1. In the **Source** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.
 2. Click **Add new address** to create a new address.
The **Create Addresses** page appears.
 3. Configure the new address. See [“Creating Addresses or Address Groups” on page 753](#).
 4. Click **Save** to save the new address.

The new address is created, and will be listed as an option for the source. Select the new address to add it to the source.

RELATED DOCUMENTATION

[Selecting NAT Destination | 652](#)

[Creating NAT Policy Rules | 638](#)

[Editing, Cloning, and Deleting NAT Policy Rules | 645](#)

[Deploying NAT Policy Rules | 647](#)

[About the Single NAT Policy Page | 636](#)

[NAT Policies Overview | 629](#)

[About the NAT Policies Page | 632](#)

[Creating NAT Policies | 633](#)

[Editing and Deleting NAT Policies | 635](#)

Selecting NAT Destination

IN THIS SECTION

- [Adding an Endpoint as NAT Destination | 652](#)
- [Selecting Interfaces when GWR Resides Inside an NFX Box | 652](#)
- [Selecting NAT Destination Using Abbreviations | 653](#)
- [Selecting a NAT Destination from the End Points Panel | 654](#)
- [Creating and Selecting a NAT Destination from the End Points Panel | 654](#)
- [Creating Addresses from Destination Field | 655](#)
- [Creating Services from Destination Field | 655](#)

The following procedures provides various methods that you can use to choose an endpoint as a NAT destination:

Adding an Endpoint as NAT Destination

View and select the destination endpoint from the complete list of addresses, interfaces, services, zones, routing instances, or ports.

1. Click the **Destination** field. A list of relevant endpoints are displayed.
2. Click the **View more results** link provided at the bottom of the destination endpoints. The complete list of addresses, interfaces, services, zones, and routing instances, is displayed in the **End Points** panel on the right.
3. (Optional) Click the edit icon to edit the address, service, or port endpoint.
4. Click check mark icon (✓) to select the endpoint as a destination.

Selecting Interfaces when GWR Resides Inside an NFX Box

The physical interfaces of an NFX box are mapped to the virtual interfaces of the Gateway Router (GWR) (vSRX) as given in [Table 198 on page 653](#). These are the default mappings provided by CSO. You may change these interface mappings based on your requirements.

Table 198: NFX and GWR Interface Mapping

NFX Physical Interface	GWR Virtual Interface
WAN 0 (ge-0/0/10)	ge-0/0/2
WAN 1 (ge-0/0/11)	ge-0/0/3
WAN 2 (xe-0/0/12)	ge-0/0/7
WAN 3 (xe-0/0/13)	ge-0/0/8
LAN-X (ge-0/0/X)	Ge-0/0/06.<vlan-id-for-X>

When you create a new NAT rule and an NFX physical interface is intended as the destination endpoint, select the respective mapped GWR interface.

Selecting NAT Destination Using Abbreviations

Enter an abbreviation in the **Destination** field to select the destination endpoint from a filtered list of destination endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of interfaces, enter **INTR** or **intr**.
- To view a filtered list of services, enter **SVCS** or **svcs**.
- To view a filtered list of zones, enter **ZONE** or **zone**.
- To view a filtered list of routing instances, enter **ROUT** or **rout**.

Click the endpoints in the filtered list to select them.

You can add a port number as a destination endpoint. To do so:

1. Enter **PORT** or **port** in **Destination**.
2. Press Tab.
3. Enter the port number and press Enter.

You can also enter a range of ports by using the separator -. For example, you can enter **10-20**.

The entered port value is selected as a destination endpoint.

You can also select the endpoint from the complete list of addresses, interfaces, services, zones, and routing instances. See [“Adding an Endpoint as NAT Destination” on page 652](#).

Selecting a NAT Destination from the End Points Panel

You can select a NAT destination endpoint from the **End Points** panel. Alternately, you can create a new NAT destination endpoint from the **End Points** panel, see [“Creating and Selecting a NAT Destination from the End Points Panel” on page 654](#).

To select a NAT destination endpoint from the **End Points** panel:

1. Click the **Destination** field.

2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, interfaces, services, zones, and routing instances.

3. (Optional) To view more information about a destination endpoint, click the details icon on the right of the endpoint. To edit the destination endpoint, click the edit icon (pencil symbol) on the right of the endpoint.

NOTE: You can only edit or view details of a destination endpoint if these options appear on right side of the endpoint when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the endpoint as a destination.

Creating and Selecting a NAT Destination from the End Points Panel

To create a new destination endpoint from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of endpoint you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to create a new endpoint.

- To create a new address, see [“Creating Addresses or Address Groups” on page 753](#).
- To create a new service, see [“Creating Services and Service Groups” on page 759](#).

After the endpoint is created, it appears in the **Endpoints** panel.

2. Click the check mark icon (✓) to add the new endpoint as a destination.

Creating Addresses from Destination Field

You can use one of the following ways to create a new address from the **Destination** and use the newly created address as a destination endpoint:

- Type the address directly in the **Destination** field. If the address is valid, it is created immediately and added as a destination endpoint.
- Create an address from the **Destination** field, using the following steps:

1. In the **Destination** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.

2. Click **Add new address** to create a new address.

The **Create Addresses** page appears.

3. Configure the new address. See [“Creating Addresses or Address Groups” on page 753](#).

4. Click **Save** to save the new address.

The new address is created, and will be listed as an option for the destination. Select the new address to add it to the destination.

Creating Services from Destination Field

To create a new service from the **Destination** field and use the newly created service as a destination endpoint:

1. In the **Destination** link, type **svcs**. The **Add new service** link appears at the bottom of the list of services.

2. Click **Add new service** to create a new service.

The **Create Services** page appears.

3. Configure the new service. See [“Creating Services and Service Groups” on page 759](#).

4. Click **Save** to save the new service.

The new service is created, and will be listed as an option for the destination. Select the new service to add it to the destination.

RELATED DOCUMENTATION

About the Single NAT Policy Page 636
Editing, Cloning, and Deleting NAT Policy Rules 645
Creating NAT Policy Rules 638
Deploying NAT Policy Rules 647
NAT Policies Overview 629
About the NAT Policies Page 632
Creating NAT Policies 633
Editing and Deleting NAT Policies 635

NAT Pools Overview

A NAT pool is a set of IP addresses that you can define and use for address translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Unlike static NAT, where there is a one-to-one mapping that includes destination IP address translation in one direction and source IP address translation in the reverse direction, with source NAT, you translate the original source IP address to an IP address in the address pool. With destination NAT, you translate the original destination address to an IP address in the address pool.

RELATED DOCUMENTATION

NAT Policies Overview 629
About the NAT Pools Page 656
Creating NAT Pools 658
Editing, Cloning, and Deleting NAT Pools 660

About the NAT Pools Page

To access this page, select **Configuration > NAT > Pools**.

Use the **NAT Pools** page to create, modify, clone, and delete NAT pools. You can filter and sort this information to get a better understanding of what you want to configure.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT pool. See [“Creating NAT Pools” on page 658](#).
- Modify, clone, or delete a NAT pool. See [“Editing, Cloning, and Deleting NAT Pools” on page 660](#).
- View unused NAT pools by selecting **More > Show Unused**. Delete unused NAT pools by selecting **More > Delete Unused Items**.
- View duplicate NAT pools. Select **More > Show Duplicates**. The **Show Duplicates** page appears, displaying duplicate NAT pools. To delete a duplicate NAT pool, select it and click the delete icon (X).
- View the details of a NAT pool by selecting **More > Detailed View**, or by right-clicking a NAT pool and select **Detailed View**.
- Search for a specific NAT pool. Click the Search icon in the top right corner of the page to search for a NAT pool. You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

[Table 199 on page 657](#) provides description of the fields on the **NAT Pools** page.

Table 199: Fields on the NAT Pools Page

Field	Description
Name	Displays the name of the NAT pool.
Pool Address	Displays the IP address of the NAT pool.
Description	Displays the description provided about the NAT pool when it was created.
Pool Type	Displays the NAT pool type. A NAT pool can be of type Source or Destination .

RELATED DOCUMENTATION

[NAT Pools Overview | 656](#)

[Creating NAT Pools | 658](#)

[Editing, Cloning, and Deleting NAT Pools | 660](#)

Creating NAT Pools

Use the **Create NAT Pools** page to create NAT pools.

To create a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

2. Click the add icon (+).

The **Create NAT Pool** page displays fields required for creating and configuring a NAT pool.

3. Complete the configuration according to the guidelines provided in [Table 200 on page 658](#).

4. Click **OK** to save the changes. A NAT pool with the configuration you provided is created.

If you want to discard your changes, click **Cancel** instead.

[Table 200 on page 658](#) provides guidelines on using the fields on the **Create NAT Pool** page.

Table 200: Fields on the Create NAT Pool Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, dashes, spaces, and underscores. Colons, and periods are not allowed, and the maximum length is 31 characters.
Description	Enter a description for the new NAT pool; maximum length is 1024 characters.
Pool Type	Select a NAT pool type to configure: <ul style="list-style-type: none"> • Source • Destination
Pool Address	Select a NAT pool address or click Add new address to create a new NAT pool address.
Routing Instance	
Site	Select the site to which the NAT pool is applicable.
Routing Instance	Select the required routing instance from the list of available routing instances for the selected site.

Table 200: Fields on the Create NAT Pool Page (*continued*)

Field	Description
Advanced	
Host Address Base	Enter the base address of the original source IP address range. The Host Address Base is used for IP address shifting.
Translation	<p>Select the translation type for the incoming traffic:</p> <ul style="list-style-type: none"> • No Translation—There is no translation required for the incoming traffic. • Port/Range—Set the global default single port range for source NAT pools with port translation. • Overload—Multiple source addresses are translated to pool addresses. If you set Overload as the translation type, the value of the Pool Address field cannot be an IP range or subnet, but it will be a single address.
Address Pooling	<p>Select a NAT address pooling behavior:</p> <ul style="list-style-type: none"> • Paired—Use this option for applications that require all sessions associated with one internal IP address to be translated to the same external IP address for multiple sessions. • Non-Paired—Use this option for applications that can be assigned IP addresses in a round-robin fashion.
Port	Enter the port number for the destination NAT pool type.
Start	Enter the start port range for the source NAT pools, if the translation type is Port/Range. The value of the port range can be any value between 1024 to 65535.
End	Enter the end port range. The value of the port range can be any value between 1024 to 65535.
Port Overloading Factor	Configure the port overloading capacity for a source NAT pool. If the factor is set to x, each translated IP address has x times the maximum number of ports available. The value of the port overloading factor can range between 2 and 32.
Address Sharing	Enable address sharing so that multiple internal IP addresses can be mapped to the same external IP address. Select this option only when the source NAT pool is configured with no port translation. When a source NAT pool has only one or a few external IP addresses available, the address sharing option with a many-to-one address mapping increases NAT resources and improves traffic.

Table 200: Fields on the Create NAT Pool Page (continued)

Field	Description
Overflow Pool Type	<p>Select a source pool to use when the current address pool is exhausted.</p> <ul style="list-style-type: none"> • Interface—Allow the egress interface IP address to support overflow. • Pool—Name of the source address pool. <ul style="list-style-type: none"> • Overflow Pool—When addresses from the original source NAT pool are exhausted, IP addresses and port numbers are allocated from the overflow pool. A user-defined source NAT pool or an egress interface can be used as the overflow pool. (When the overflow pool is used, the pool ID is returned with the address.)

RELATED DOCUMENTATION

[NAT Pools Overview | 656](#)

[About the NAT Pools Page | 656](#)

[Editing, Cloning, and Deleting NAT Pools | 660](#)

Editing, Cloning, and Deleting NAT Pools

IN THIS SECTION

- [Editing NAT Pools | 660](#)
- [Cloning NAT Pools | 661](#)
- [Deleting NAT Pools | 661](#)

Editing NAT Pools

To modify the parameters configured for a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

2. Select the NAT pool that you want to edit, and click the edit icon (pencil symbol) at the top right corner of the table, or right-click and select **Edit NAT Pool**.

The **Edit NAT Pool** page appears, displaying the same options that are displayed when creating a new NAT pool.

3. Modify the parameters according to the guidelines provided in [“Creating NAT Pools” on page 658](#).
4. Click **OK** to save the changes. If you click **OK**, you see the modified NAT pool in the **NAT Pools** page.
If you want to discard your changes, click **Cancel** instead.

Cloning NAT Pools

To clone a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

2. Right-click the NAT pool that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone NAT Pool** page appears with editable fields. Modify the parameters of the cloned NAT pool as per your requirements.

3. Click **OK** to save the changes. If you click **OK**, the cloned NAT pool appears at the end of the NAT pools list in the **NAT Pools** page.
If you want to discard your changes, click **Cancel** instead.

Deleting NAT Pools

To delete a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

2. Select the NAT pool you want to delete and then click the delete icon **(X)**.

An alert message appears, verifying that you want to delete the NAT pool.

3. Click **Yes** to delete the NAT pool. If you click **Yes**, the selected NAT pool is deleted.
If you do not want to delete, click **Cancel** instead.

RELATED DOCUMENTATION

[NAT Pools Overview | 656](#)

[About the NAT Pools Page | 656](#)

[Creating NAT Pools | 658](#)

Deploying NAT Policies

After adding the intents to the NAT policies, you can deploy the NAT policy by clicking the **Deploy** option that is above the **End Points** panel. You can also deploy one or more policies from the **NAT Policies** page.

To deploy NAT policies:

1. Select **Configuration > NAT > NAT Policies**.

The NAT Policies page appears.

2. Select one or more policies and click **Deploy**.

The Deploy page appears.

3. In **Choose Deployment Time** options, select **Run Now** to deploy the policy immediately. Select **Schedule at a later time** and specify the date and time at which the policy should be deployed.

4. Click **Deploy**.

A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

Importing NAT Policies

Use this page to manually import a firewall policy from the discovered or onboarded sites (next generation firewall sites).

To import a NAT policy:

1. Select **Configuration > NAT > NAT Policies**.

The NAT Policy page appears.

2. Click **Import**.

The Import NAT Policies page appears displaying a list of discovered devices (next generation firewall devices).

3. Select the devices from which you want to import the NAT policies and click **Next**.

The Discovered Services tab appears.

4. Select the NAT policies that you want to import and click **Next**.

The Resolve Conflicts tab appears.

5. If there are any conflicts with the imported objects, object conflict resolution(OCR) operation is triggered. The Conflicts window displays all the conflicts between CSO and the next generation firewall device. Select an object from the Conflicts window and click on any of the below option to resolve the object conflict.

The resolution options are:

- **Rename Object**—Rename the imported object. By default, "_1" is added to the object name, or you can specify a new name.
- **Overwrite with imported value**—The object in CSO is replaced with the object from the import operation.
- **Keep existing object**—The object name in CSO is used instead of what is on the next generation firewall device.

6. Click **Finish**.

A summary of the discovered services is listed.

7. Review the summary and click **OK** to import the NAT policies.

The import policy job is created and the NAT policies are imported from next generation firewall device to CSO. You can view the imported policy from the NAT Policies page.

WHAT'S NEXT

After importing the NAT policy successfully, you can edit and deploy the policy. See [Editing and Deleting NAT Policies | 635](#), [Editing, Cloning, and Deleting NAT Pools | 660](#), and [Deploying NAT Policies | 662](#).

RELATED DOCUMENTATION

| [Importing Policies Overview](#) | 514

Managing IPS Signatures and Profiles

IN THIS CHAPTER

- [About the IPS Signatures Page | 665](#)
- [Create IPS Signatures | 670](#)
- [Create IPS Signature Static Groups | 678](#)
- [Create IPS Signature Dynamic Groups | 679](#)
- [Edit, Clone, and Delete IPS Signatures | 685](#)
- [Edit, Clone, and Delete IPS Signature Static Groups | 687](#)
- [Edit, Clone, and Delete IPS Signature Dynamic Groups | 690](#)
- [About the IPS Profiles Page | 692](#)
- [Create IPS Profiles | 694](#)
- [Edit, Clone, and Delete IPS Profiles | 695](#)
- [About the <IPS-Profile-Name> / Rules Page | 697](#)
- [Create IPS or Exempt Rules | 699](#)
- [Edit, Clone, and Delete IPS or Exempt Rules | 707](#)

About the IPS Signatures Page

IN THIS SECTION

- [Tasks You Can Perform | 666](#)
- [Field Descriptions | 666](#)

To access this page, select **Configure > IPS > IPS Signature**.

Use intrusion prevention system (IPS) signatures to monitor and prevent intrusions. IPS compares traffic against signatures of known threats and blocks traffic when a threat is detected.

Tasks You Can Perform

- View the details of an IPS signature—Select an IPS signature and click **More > Details**, or mouse over the IPS signature and click the **Detailed View** icon. The IPS Signature Details View page appears. See [Table 202 on page 668](#) for an explanation of fields on this page.
- View the details of an IPS signature static group—Select an IPS signature static group and click **More > Details**, or mouse over the IPS signature static group and click the **Detailed View** icon. The IPS Static Group Details page appears. See [Table 203 on page 669](#) for an explanation of fields on this page.
- View the details of an IPS signature dynamic group—Select an IPS signature dynamic group and click **More > Details**, or mouse over the IPS signature dynamic group and click the **Detailed View** icon. The IPS Signature Dynamic Details View page appears. See [Table 204 on page 669](#) for an explanation of fields on this page.
- Create an IPS signature—See [“Create IPS Signatures” on page 670](#).
- Create an IPS signature static group—See [“Create IPS Signature Static Groups” on page 678](#).
- Create an IPS signature dynamic group—See [“Create IPS Signature Dynamic Groups” on page 679](#).
- Edit, clone, or delete an IPS signature—See [“Edit, Clone, and Delete IPS Signatures” on page 685](#).
- Edit, clone, or delete an IPS signature static group—See [“Edit, Clone, and Delete IPS Signature Static Groups” on page 687](#).
- Edit, clone, or delete an IPS signature dynamic group—See [“Edit, Clone, and Delete IPS Signature Dynamic Groups” on page 690](#).
- Search for IPS signatures, static groups or dynamic groups by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Filter IPS signatures, static groups or dynamic groups—Click the filter icon (funnel) and specify one or more filtering criteria. The filtered results are displayed on the same page.
- Sort IPS signatures, static groups or dynamic groups—Click a column name to sort the data in the grid (table) based on the column name.

NOTE: Sorting is applicable only to some fields.

- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the page.

Field Descriptions

[Table 201 on page 667](#) describes the field on the IPS Signatures page.

Table 201: Fields on the IPS Signatures Page

Field	Description
Name	Name of the IPS signature, IPS signature static group, or IPS signature dynamic group.
Severity	Severity level of the attack that the signature will report.
Category	Category of the attack object.
Object Type	Displays the type of attack object: <ul style="list-style-type: none"> • Static Group • Dynamic Group • Signature • Protocol Anomaly • Compound Attack
Recommended	Indicates whether the attack objects are recommended by Juniper (True) or not (False).
Action	Action taken when the monitored traffic matches the attack objects specified in the IPS rules.
Definition Type	Displays whether the IPS signature, static group, or dynamic group was created by CSO (Predefined) or user-created (Custom).
CVE	Displays the Common Vulnerabilities and Exposures (CVE) identifier or name associated with the threat.
CERT	Displays the computer emergency response team (CERT) advisory number associated with the threat.
BUG	Displays the list of bugs that are related to the signature attack.
False Positives	Displays the frequency with which the attack produces a false positive on your network.
Service	Protocol or service that the attack uses to enter your network.
Performance Impact	Performance impact of the IPS signature.
Direction	Direction of the traffic for which the attack is detected; for example, client to server.

Table 202: Fields on the IPS Signature Details View Page

Field	Description
Name	Name of the IPS signature.
Description	Description of the IPS signature.
URL(s)	Displays the URLs that have the details about the signature attack. For example, http://www.faqs.org/rfcs/rfc2865.html .
Category	See Table 201 on page 667 .
Recommended	See Table 201 on page 667 .
Action	See Table 201 on page 667 .
Keywords	Keywords associated with the IPS signature.
Severity	See Table 201 on page 667 .
BUGS	See Table 201 on page 667 .
CERT	See Table 201 on page 667 .
CVE	See Table 201 on page 667 .
<i>Signature Details</i>	
Binding	Protocol or service that the attack uses to enter your network.
Service	For service binding, displays the service the attack uses to enter your network.
Time Count	Number of time that IPS detects the attack in a specified time scope.

Table 202: Fields on the IPS Signature Details View Page (*continued*)

Field	Description
Signature	<p>Displays (in a table) the signature attack objects configured as part of the IPS signature. For each row, the following fields are displayed:</p> <ul style="list-style-type: none"> • No.—Unique identifier for the signature attack object. • Context—Attack context, which defines the location of the signature where IPS should look for the attack. • Direction—Connection direction of the attack. • Pattern—Signature pattern (in Juniper's proprietary regular expression syntax) of the attack to be detected. • Regex—Regular expression to match malicious or unwanted behavior over the network. • Negated—Indicates whether the pattern should be excluded from being matched (true) or not (false).
Anomaly	<p>Displays (in a table) the protocol anomaly attack objects configured as part of the IPS signature. For each row, the following fields are displayed:</p> <ul style="list-style-type: none"> • No.—Unique identifier for the anomaly. • Anomaly—Protocol or service for which the anomaly is defined. • Direction—Connection direction of the attack.

Table 203: Fields on the IPS Static Group Details Page

Field	Description
Name	Name of the IPS signature static group.
Description	Description of the IPS signature static group.
Group Members	<p>Displays the IPS signatures or IPS signature dynamic groups that are part of the IPS static group. See Table 201 on page 667 for an explanation of the fields in the table.</p> <p>To view the details, select a row, click More > Details, or mouse over a row and click the Detailed View icon. Depending on the object type, the IPS Signature Details View page or IPS Signature Dynamic Details View page appears. See Table 202 on page 668 and Table 204 on page 669 for an explanation of the fields on these pages.</p>

Table 204: Fields on the IPS Signature Dynamic Details View Page

Field	Description
Name	Name of the IPS signature dynamic group.

Table 204: Fields on the IPS Signature Dynamic Details View Page (*continued*)

Field	Description
Severity	Severity filters used for the dynamic group.
Service	Services filters used for the dynamic group.
Category	Category filters used for the dynamic group.
Recommended	Indicates whether predefined attack objects recommended by Juniper are added to the dynamic group (true) or not (false).
Direction	Traffic direction (for which the attack is detected) filters used for the dynamic group.
Performance Impact	Performance impact filter used for the dynamic group.
False Positive	False positive filter used for the dynamic group.
Age of Attack	Age of the attack (in years) used as a filter for the dynamic group.
CVSS Score	Common Vulnerability Scoring System (CVSS) score used as a filter for the dynamic group.
File Type	File type of the attack used as a filter for the dynamic group.
Vulnerability Type	Vulnerability type of the attack used as a filter for the dynamic group.
Object Type	Type of object (anomaly or signature) used as a filter for the dynamic group.
Vendor Description	Vendor or product that the attack belongs to.

RELATED DOCUMENTATION

[About the IPS Profiles Page](#) | [692](#)

Create IPS Signatures

The signature database in Contrail Service Orchestration (CSO) contains predefined intrusion prevention system (IPS) signatures that you can use. From the Create IPS Signature page, users with the tenant

administrator role or a custom role with appropriate IPS tasks can also create customized IPS signatures to block newer attacks or unknown attacks.

To create a customized IPS signature:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select **Create > IPS Signature**.

The Create IPS Signature page appears.

3. Complete the configuration according to the guidelines in [Table 205 on page 671](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the IPS Signatures page and a message indicating that the signature is created is displayed.

After you create an IPS signature, you can use the signature in an IPS or an exempt rule and reference the IPS profile (containing the rule) in a firewall policy that you can then deploy on the device.

Table 205: Create IPS Signature Settings

Setting	Guideline
Name	Enter a unique name for the IPS signature that is a string of alphanumeric characters and some special characters (colon, hyphen, period, and underscore). No spaces are allowed and the maximum length is 255 characters.
Description	Enter a description for the IPS signature; the maximum length is 1024 characters.
Category	<p>Enter a predefined category or a new category. The category can contain alphanumeric characters and special characters (hyphen and underscore) and must begin with an alphanumeric character. No spaces are allowed and the maximum length is 63 characters.</p> <p>You use categories to group attack objects and then within each category, you can assign severity levels to the attack objects.</p>

Table 205: Create IPS Signature Settings (*continued*)

Setting	Guideline
Action	<p>Select the action to take when the monitored traffic matches the attack objects specified in the IPS rule:</p> <ul style="list-style-type: none"> • None—No action is taken. Use this action to only generate logs for some traffic. • Close Client & Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. • Drop—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.
Keywords	<p>Enter unique identifiers that can be used to search and sort signatures. Keywords should relate to the attack and the attack object. For example, Amanda Aminindexd Remote Overflow.</p>
Severity	<p>Select a severity level for the attack that the signature will report:</p> <ul style="list-style-type: none"> • Critical—Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges. • Major—Contains attack objects matching exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device. • Minor—Contains attack objects matching exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks. • Warning—Contains attack objects matching exploits that attempt to obtain noncritical information or scan a network with a scanning tool. • Info—Contains attack objects matching normal, harmless traffic containing URLs, DNS lookup failures, SNMP public community strings, and peer-to-peer (P2P) parameters. You can use informational attack objects to obtain information about your network.
<i>Signature Details</i>	

Table 205: Create IPS Signature Settings (*continued*)

Setting	Guideline
Binding	<p>Select the protocol or service that the attack uses to enter your network:</p> <ul style="list-style-type: none"> • IP—Match the attack for a specified protocol type number, which you must specify in the Protocol field. • IPv6—Match the attack for a specified protocol type number (for the header following the IPv6 header), which you must specify in the Next Header field • ICMP—Match the attack for ICMP packets. • IPv6—Match the attack for ICMPv6 packets. • TCP—Match the attack for specified TCP ports or port ranges, which you must specify in the Port Range(s) field. • UDP—Match the attack for specified UDP ports or port ranges. • RPC—Match the attack for a specified remote procedure call (RPC) program number, which you must specify in the Program Number field. • Service—Match the attack for a specified service, which you must choose from the Service field.
Protocol	<p>For IP binding, specify the transport layer protocol number that you want matched to the attack.</p> <p>Range: 1 through 139 excluding 1, 6, and 17.</p>
Next Header	<p>For IPv6 binding, specify the transport layer protocol number for the next header following the IPv6 header with which to match the attack.</p> <p>Range: 1 through 139 excluding 6, 17, and 58.</p>
Port Range(s)	<p>For TCP or UDP binding, specify a port number or a port range (<i>min-port-no-max-port-no</i> format) that you want matched to the attack.</p>
Program Number	<p>For RPC binding, specify the RPC program number (ID) that you want matched to the attack.</p>
Service	<p>For service binding, select the service that you want matched to the attack.</p>
Time Count	<p>Specify the number of times that IPS detects the attack within the specified time scope before triggering an event.</p>

Table 205: Create IPS Signature Settings (*continued*)

Setting	Guideline
Time Scope	<p>Specify the scope within which the counting of the attack occurs:</p> <ul style="list-style-type: none"> • Source IP—Detect attacks from the source IP address for the specified time count regardless of the destination IP address. • Dest IP—Detect attacks from the destination IP address for the specified time count regardless of the source IP address. • Peer—Detect attacks between source and destination IP addresses of the sessions for the specified time count.
Match Assurance	<p>Specify a false positives filter to track attack objects based on the frequency that the attack produces a false positive on your network:</p> <ul style="list-style-type: none"> • High—Provides information on the frequently tracked false positive occurrences. • Medium—Provides information on the occasionally tracked false positive occurrences. • Low—Provides information on the rarely tracked false positive occurrences.
Performance Impact	<p>Specify this filter to select only the appropriate attacks based on performance impact; for example to filter out slow-performing attack objects:</p> <ul style="list-style-type: none"> • High—Add high performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is high7 to high9, where the application identification is slow. • Medium—Add medium performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is medium4 to medium6, where the application identification is normal. • Low—Add low performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is low1 to low3, where the application identification is faster. • Unknown—Add attack objects whose performance impact is unknown.

Table 205: Create IPS Signature Settings (continued)

Setting	Guideline
Add Signature	<p>You can specify one or more signature attack objects that use a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks.</p> <p>NOTE: For a customized IPS signature, you must specify at least one signature attack object or anomaly.</p> <ul style="list-style-type: none">• To add a signature attack object:<ol style="list-style-type: none">1. Click the add (+) icon.<p>The Add Signature page appears.</p>2. Complete the configuration according to the guidelines in Table 206 on page 677.3. Click OK.<p>You are returned to the previous page and the signature attack object is displayed in the table.</p>• To modify a signature attack object that you added:<ol style="list-style-type: none">1. Select an attack object and click the edit (pencil) icon.<p>The Edit Signature page appears, displaying the same fields that appear when you add a signature attack object.</p>2. Modify the fields as needed. See Table 206 on page 677.3. Click OK.<p>Your modifications are saved and you are returned to the previous page.</p>• To delete a signature attack object that you added:<ol style="list-style-type: none">1. Select an attack object and click the delete (trash can) icon.<p>A popup appears asking you to confirm the delete operation.</p>2. Click Yes.<p>The signature attack object is deleted and you are returned to the previous page.</p>

Table 205: Create IPS Signature Settings (*continued*)

Setting	Guideline
Add Anomaly	<p>NOTE:</p> <ul style="list-style-type: none"> The Add Anomaly field is displayed only if you specify a service binding. For a customized IPS signature, you must specify at least one signature attack object or anomaly. <p>Protocol anomaly attack objects detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used.</p> <p>You can add, modify, or delete anomaly attack objects:</p> <ul style="list-style-type: none"> To add an anomaly: <ol style="list-style-type: none"> Click the add (+) icon. The Add Anomaly page appears. Complete the configuration according to the guidelines in Table 207 on page 677. Click OK. You are returned to the previous page and the anomaly is displayed in the table. To modify an anomaly that you added: <ol style="list-style-type: none"> Select an anomaly and click the edit (pencil) icon. The Edit Anomaly page appears, displaying the same fields that appear when you add an anomaly. Modify the fields as needed. See Table 207 on page 677. Click OK. Your modifications are saved and you are returned to the previous page. To delete an anomaly that you added: <ol style="list-style-type: none"> Select an anomaly and click the delete (trash can) icon. A popup appears asking you to confirm the delete operation. Click Yes. The signature anomaly is deleted and you are returned to the previous page.

Table 206: Add Signature Settings

Setting	Guideline
Signature No.	Displays the system-generated signature number; you cannot modify this field.
Context	Select the attack context, which defines the location of the signature where IPS should look for the attack in a specific Application Layer protocol.
Direction	<p>Select the connection direction of the attack:</p> <ul style="list-style-type: none"> • Any—Detect the attack for traffic in either direction. • Client to-Server—Detect the attack only in client-to-server traffic. • Server to Client—Detect the attack only in server to client traffic.
Pattern	<p>Enter the signature pattern (in Juniper Networks proprietary regular expression syntax) of the attack you want to detect.</p> <p>An attack pattern can be a segment of code, a URL, or a value in a packet header and the signature pattern is the syntactical expression that represents that attack pattern.</p> <p>For example, use <code>\[<character-set>\]</code> for case-insensitive matches.</p>
Regex	Enter a regular expression to define rules to match malicious or unwanted behavior over the network. For example: For the syntax <code>\[hello\]</code> , the expected pattern is hello, which is case sensitive. The example matches can be: hElLo, HEIIO, and heLLO.
Negated	Select this check box to exclude the specified pattern from being matched. When you negate a pattern, the attack is considered matched if the pattern defined in the attack does not match the specified pattern.

Table 207: Add Anomaly Settings

Setting	Guideline
Anomaly No.	Displays the system-generated anomaly number; you cannot modify this field.
Anomaly	Select the protocol (service) whose anomaly is being defined in the attack.
Direction	<p>Select the connection direction of the attack:</p> <ul style="list-style-type: none"> • Any—Detect the attack for traffic in either direction. • Client to-Server—Detect the attack only in client-to-server traffic. • Server to Client—Detect the attack only in server to client traffic.

RELATED DOCUMENTATION

| [Create IPS Profiles](#) | 694

Create IPS Signature Static Groups

The signature database in Contrail Service Orchestration (CSO) contains predefined intrusion prevention system (IPS) signature static groups that you can use. Users with the tenant administrator role or a custom role with appropriate IPS tasks can also create customized IPS signature static groups from the Create IPS Signature Static Group page. Static groups enable better manageability because you can group different types of signatures into one entity.

To create a customized IPS signature static group:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select **Create > Static Group**.

The Create IPS Signature Static Group page appears.

3. Complete the configuration according to the guidelines in [Table 208 on page 678](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the IPS Signatures page and a message that the static group was successfully created is displayed.

After you create an IPS signature static group, you can use the static group in an IPS or an exempt rule and reference the IPS profile (containing the rule) in a firewall policy that you can then deploy on the device.

Table 208: Create IPS Signature Static Group Settings

Setting	Guideline
Name	Enter a unique name for the IPS signature static group that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.

Table 208: Create IPS Signature Static Group Settings (continued)

Setting	Guideline
Description	Enter a description for the IPS signature static group; the maximum length is 1024 characters.
Group Members	<p>You can add one or more IPS signatures, static groups, or dynamic groups to be members of the static group that you are creating. In addition, you can delete group members after adding them.</p> <p>NOTE: You must add at least one IPS signature, static group, or dynamic group to proceed.</p> <ul style="list-style-type: none"> To add one or more group members: <ol style="list-style-type: none"> Click the add (+) icon. <p>The Add IPS Signatures page appears displaying the existing predefined and custom IPS signatures, static groups, and dynamic groups in a table..</p> Select one or more group members by clicking the check boxes corresponding to the rows. Click OK. <p>You are returned to the previous page and the group members that you added are displayed in the table.</p> To delete one or more group members that you added: <ol style="list-style-type: none"> Select the group members that you want to delete and click the delete (trash can) icon. <p>A warning message appears asking you to confirm the deletion.</p> Click Yes. <p>The group members are deleted.</p>

RELATED DOCUMENTATION

| [Create IPS Profiles](#) | 694

Create IPS Signature Dynamic Groups

The signature database in Contrail Service Orchestration (CSO) contains predefined intrusion prevention system (IPS) signature dynamic groups that you can use. Users with the tenant administrator role or a

custom role with appropriate IPS tasks can also create customized IPS signature dynamic groups (based on a specified filter criteria) from the Create IPS Signature Dynamic Group page.

The filter criteria that you specify are matched only to predefined or customized IPS signatures, and not to IPS static groups dynamic groups. When a new signature database is used, the dynamic group membership is automatically updated based on the filter criteria for that group.

To create a customized IPS signature dynamic group:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select **Create > Dynamic Group**.

The Create IPS Signature Static Group page appears.

3. Complete the configuration according to the guidelines in [Table 209 on page 680](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. (Optional) Click **Preview Filtered Signatures** to check if the signatures that match the dynamic group are consistent with the filter criteria that you specified.

The IPS Signatures page appears displaying the list of IPS signatures matching the filters. If the signatures do not match, you can tweak the filter criteria as needed. Click **Close** to go back to the previous page.

5. Click **OK**.

You are returned to the IPS Signatures page and a message indicating that the dynamic group was successfully created is displayed.

After you create an IPS signature dynamic group, you can use the dynamic group in an IPS or an exempt rule and reference the IPS profile (containing the rule) in a firewall policy that you can then deploy on the device.

Table 209: Create IPS Signature Dynamic Group Settings

Setting	Guideline
Name	Enter a unique name for the IPS signature dynamic group that is a string of alphanumeric characters, colons, periods, hyphens, and underscores. No spaces are allowed and the maximum length is 255 characters.

Table 209: Create IPS Signature Dynamic Group Settings (*continued*)

Setting	Guideline
<i>Filter Criteria</i>	<p>You select one or more filters to define the attributes of IPS signatures that will be added to the IPS signature dynamic group that you are creating. Filters apply to existing signatures (already downloaded in CSO) and to new signatures when they are downloaded.</p> <p>IPS signatures that match any of the filters that you configure are included as part of the signature group.</p>
Severity	
Info	Select the Enable check box to include IPS signatures with the severity level Info.
Warning	Select the Enable check box to include IPS signatures with the severity level Warning.
Minor	Select the Enable check box to include IPS signatures with the severity level Minor.
Major	Select the Enable check box to include IPS signatures with the severity level Major.
Critical	Select the Enable check box to include IPS signatures with the severity level Critical.
<i>Service</i>	
Service	<p>Specify the services that you want to use to filter for IPS signatures that should be included as part of the dynamic group.</p> <p>Select one or more services listed in the Available column and click the forward arrow to confirm your selection. The selected services are displayed in the Selected column.</p>
<i>Category</i>	
Category	<p>Specify the categories that you want to use to filter for IPS signatures that should be included as part of the dynamic group.</p> <p>Select one or more categories listed in the Available column and click the forward arrow to confirm your selection. The selected categories are displayed in the Selected column.</p>
<i>Recommended</i>	

Table 209: Create IPS Signature Dynamic Group Settings (*continued*)

Setting	Guideline
Recommended	<p>This filter is based on attack objects recommended by Juniper Networks. Select one of the following:</p> <ul style="list-style-type: none"> • None—Don't use this filter. • Yes—Add predefined attacks recommended by Juniper Networks to the dynamic group. • No—Add predefined attacks that are not recommended by Juniper Networks to the dynamic group.
<i>Direction</i>	<p>You use this filter to add IPS signatures to the dynamic group based on the traffic direction of the attacks.</p> <p>If you specify more than one traffic direction (Any, Client-to-Server, and Server-to-Client), you must select a value in the Expression field.</p>
Any	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None (default): Do not use this filter. • Yes: Include IPS signatures that track traffic from client to server or server to client. • No: Do not include IPS signatures that track traffic from client to server or server to client.
Client-to-Server	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None (default): Do not use this filter. • Yes: Include IPS signatures that track traffic from client to server. • No: Do not include IPS signatures that track traffic from client to server.
Server-to-Client	<p>Select one of the following:.</p> <ul style="list-style-type: none"> • None (default): Do not use this filter • Yes: Include IPS signatures that track traffic from server to client. • No: Do not include IPS signatures that track traffic from server to client.
Expression	<p>If you specified more than one direction filter, you must specify how the signatures should be matched:</p> <ul style="list-style-type: none"> • OR—Include signatures that match any of the specified traffic directions. • AND—Include signatures that match all of the specified traffic directions.
<i>Performance Impact</i>	

Table 209: Create IPS Signature Dynamic Group Settings (*continued*)

Setting	Guideline
Unknown	Select the Enable check box to include IPS signatures with the performance impact Unknown.
Low	Select the Enable check box to include IPS signatures with the performance impact Low.
Medium	Select the Enable check box to include IPS signatures with the performance impact Medium.
High	Select the Enable check box to include IPS signatures with the performance impact High.
<i>False Positives</i>	
Unknown	Select the Enable check box to include IPS signatures with the match assurance Unknown.
Low	Select the Enable check box to include IPS signatures with the match assurance Low.
Medium	Select the Enable check box to include IPS signatures with the match assurance Medium.
High	Select the Enable check box to include IPS signatures with the match assurance High.
<i>Age of Attack</i>	
Age of Attack	<p>Enter the age of the attack (in years) to be used as a filter criteria to include IPS signatures as part of the dynamic group.</p> <p>Range: 1 through 100.</p>
Expression	Select whether the IPS signatures should be filtered based on whether the age of attack in the signature is greater than (default) or less than the value that you specified.
<i>CVSS Score</i>	

Table 209: Create IPS Signature Dynamic Group Settings (*continued*)

Setting	Guideline
CVSS Score	<p>Specify the Common Vulnerability Scoring System (CVSS) to be used as a filter criteria to include IPS signatures as part of the dynamic group.</p> <p>Range: Decimal number between 0 and 10.</p>
Expression	Select whether the IPS signatures should be filtered based on whether the CVSS score of the attack is greater than (default) or less than the value that you specified.
<i>Other Filters</i>	
Excluded	<p>Select one of the following:.</p> <ul style="list-style-type: none"> • None (default): Do not use this filter • Yes: Include excluded attack objects as part of the dynamic group. • No: Do not include excluded attack objects as part of the dynamic group.
File Type	Select the file type of the attack to be used as a filter criteria; for example, flash.
Vulnerability Type	Select the vulnerability type of the attack to be used as a filter criteria; for example, overflow.
<i>Object Type</i>	Specify this filter to group attack objects by type (anomaly or signature).
Signature	<p>Select the Enable check box to add signatures based on stateful signature attack objects specified in the signature.</p> <p>A stateful attack signature is a pattern that always exists within a specific section of the attack. Stateful signature attack objects also include the protocol or service used to perpetrate the attack and the context in which the attack occurs.</p>
Protocol Anomaly	Select the Enable check box to add signatures of attacks that violate protocol specifications (RFCs and common RFC extensions).
<i>Vendor Description</i>	
Product Type	Specify this filter to include signatures belonging to the selected product type.
Vendor Name	Specify this filter to include signatures belonging to the selected vendor.
Title	<p>Specify this filter to include signatures belonging to the selected product name.</p> <p>The product names are populated only when you select a product type and a vendor.</p>

RELATED DOCUMENTATION

[Create IPS Profiles](#) | 694

Edit, Clone, and Delete IPS Signatures

IN THIS SECTION

- [Edit IPS Signatures](#) | 685
- [Clone IPS Signatures](#) | 686
- [Delete IPS Signatures](#) | 686

Users with the tenant administrator role or a custom role with appropriate IPS tasks can edit, clone, or delete IPS signatures.

Edit IPS Signatures

You can edit only customized IPS signatures and not predefined (system-generated) signatures.

To edit a customized IPS signature:

1. Select **Configuration** > **IPS** > **IPS Signatures**.

The IPS Signatures page appears.

2. Select a customized IPS signature and click the edit (pencil) icon.

The Edit IPS Signature page appears, displaying the same fields that are presented when you create an IPS signature.

3. Modify the IPS signature fields as needed. See [“Create IPS Signatures” on page 670](#).

NOTE: You can modify all fields except the name.

4. Click **OK** to save your changes.

You are returned to the IPS Signatures page and a message that the IPS signature was successfully updated is displayed.

If the IPS signature was used in an IPS or exempt rule that is deployed on the device (through the firewall policy), then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone IPS Signatures

Cloning enables you to easily create a new IPS signature based on an existing one. You can clone predefined or customized IPS signatures and modify the parameters as needed.

To clone an IPS signature:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select an IPS signature and select **More > Clone**.

The Clone IPS Signature page appears, displaying the same fields that are presented when you create an IPS signature.

3. Modify the IPS signature fields as needed. See [“Create IPS Signatures” on page 670](#).

4. Click **OK** to save your changes.

You are returned to the IPS Signatures page and a message that the IPS signature was successfully created is displayed.

After you clone an IPS signature, you can use the signature in an IPS or an exempt rule and reference the IPS profile (containing the rule) in a firewall policy that you can then deploy on the device.

Delete IPS Signatures

NOTE:

- You can delete only customized (user-created) IPS signatures that are not used in an IPS or exempt rule.
- You cannot delete predefined (system-generated) IPS signatures.

To delete one or more customized IPS signatures:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select one or more customized IPS signatures and click the delete (trash can) icon

A warning message appears asking you to confirm the deletion.

3. Click **Yes** to proceed with the deletion.

You are returned to the IPS Signatures page and a message indicating the status of the delete operation is displayed.

RELATED DOCUMENTATION

| [Create IPS Profiles | 694](#)

Edit, Clone, and Delete IPS Signature Static Groups

IN THIS SECTION

- [Edit IPS Signature Static Groups | 687](#)
- [Clone IPS Signature Static Groups | 688](#)
- [Delete IPS Signature Static Groups | 689](#)

Users with the tenant administrator role or a custom role with appropriate IPS tasks can edit, clone, or delete IPS signature static groups.

Edit IPS Signature Static Groups

You can edit only customized IPS signature static groups and not predefined (system-generated) static groups.

To edit a customized IPS signature static group:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select a customized IPS signature static group and click the edit (pencil) icon.

The Edit IPS Signature Static Group page appears, displaying the same fields that are presented when you create an IPS signature static group.

3. Modify the IPS signature static group fields as needed. See [“Create IPS Signature Static Groups” on page 678](#).

NOTE: You can modify all fields except the name.

4. Click **OK** to save your changes.

You are returned to the IPS Signatures page and a message that the IPS signature static group was successfully updated is displayed.

If the IPS signature static group was used in an IPS or exempt rule that is deployed on the device (through the firewall policy), then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone IPS Signature Static Groups

Cloning enables you to easily create a new IPS signature static group based on an existing one. You can clone predefined or customized IPS signature static groups and modify the parameters as needed.

To clone an IPS signature static group:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select an IPS signature static group and select **More > Clone**.

The Clone IPS Signature Static Group page appears, displaying the same fields that are presented when you create an IPS signature static group.

3. Modify the IPS signature static group fields as needed. See [“Create IPS Signature Static Groups” on page 678](#).
4. Click **OK** to save your changes.

You are returned to the IPS Signatures page and a message that the IPS signature static group was successfully created is displayed.

After you clone an IPS signature static group, you can use the static group in an IPS or an exempt rule and reference the IPS profile (containing the rule) in a firewall policy that you can then deploy on the device.

Delete IPS Signature Static Groups

NOTE:

- You can delete only customized (user-created) IPS signature static groups that are not used in an IPS or exempt rule.
- You cannot delete predefined (system-generated) IPS signature static groups.

To delete one or more customized IPS signature static groups:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select one or more customized IPS signature static groups and click the delete (trash can) icon

A warning message appears asking you to confirm the deletion.

3. Click **Yes** to proceed with the deletion.

You are returned to the IPS Signatures page and a message indicating the status of the delete operation is displayed.

RELATED DOCUMENTATION

[Create IPS Profiles](#) | 694

Edit, Clone, and Delete IPS Signature Dynamic Groups

IN THIS SECTION

- [Edit IPS Signature Dynamic Groups | 690](#)
- [Clone IPS Signature Dynamic Groups | 691](#)
- [Delete IPS Signature Dynamic Groups | 692](#)

Users with the tenant administrator role or a custom role with appropriate IPS tasks can edit, clone, or delete IPS signature dynamic groups.

Edit IPS Signature Dynamic Groups

You can edit only customized IPS signature dynamic groups and not predefined (system-generated) dynamic groups.

To edit a customized IPS signature dynamic group:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select a customized IPS signature dynamic group and click the edit (pencil) icon.

The Edit IPS Signature Dynamic Group page appears, displaying the same fields that are presented when you create an IPS signature dynamic group.

3. Modify the IPS signature dynamic group fields as needed. See [“Create IPS Signature Dynamic Groups” on page 679](#).

NOTE: You can modify all fields except the name.

4. (Optional) Click **Preview Filtered Signatures** to check if the signatures that match the dynamic group are consistent with the filter criteria that you specified.

The IPS Signatures page appears displaying the list of IPS signatures matching the filters. If the signatures do not match, you can tweak the filter criteria as needed. Click **Close** to go back to the previous page.

5. Click **OK** to save your changes.

You are returned to the IPS Signatures page and a message indicating that the IPS signature dynamic group was successfully updated is displayed.

If the IPS signature dynamic group was used in an IPS or exempt rule that is deployed on the device (through the firewall policy), then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone IPS Signature Dynamic Groups

Cloning enables you to easily create a new IPS signature dynamic group based on an existing one. You can clone predefined or customized IPS signature dynamic groups and modify the parameters as needed.

To clone an IPS signature dynamic group:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select an IPS signature dynamic group and select **More > Clone**.

The Clone IPS Signature Dynamic Group page appears, displaying the same fields that are presented when you create an IPS signature dynamic group.

3. Modify the IPS signature dynamic group fields as needed. See [“Create IPS Signature Dynamic Groups” on page 679](#).

4. (Optional) Click **Preview Filtered Signatures** to check if the signatures that match the dynamic group are consistent with the filter criteria that you specified.

The IPS Signatures page appears displaying the list of IPS signatures matching the filters. If the signatures do not match, you can tweak the filter criteria as needed. Click **Close** to go back to the previous page.

5. Click **OK** to save your changes.

You are returned to the IPS Signatures page and a message that the IPS signature dynamic group was successfully created is displayed.

After you clone an IPS signature dynamic group, you can use the dynamic group in an IPS or an exempt rule and reference the IPS profile (containing the rule) in a firewall policy that you can then deploy on the device.

Delete IPS Signature Dynamic Groups

NOTE:

- You can delete only customized (user-created) IPS signature dynamic groups that are not used in an IPS or exempt rule.
- You cannot delete predefined (system-generated) IPS signature dynamic groups.

To delete one or more customized IPS signature dynamic groups:

1. Select **Configuration > IPS > IPS Signatures**.

The IPS Signatures page appears.

2. Select one or more customized IPS signature dynamic groups and click the delete (trash can) icon

A warning message appears asking you to confirm the deletion.

3. Click **Yes** to proceed with the deletion.

You are returned to the IPS Signatures page and a message indicating the status of the delete operation is displayed.

RELATED DOCUMENTATION

| [Create IPS Profiles](#) | 694

About the IPS Profiles Page

IN THIS SECTION

- [Tasks You Can Perform](#) | 693
- [Field Descriptions](#) | 693

To access this page, select **Configure > IPS > IPS Profiles**.

Use intrusion prevention system (IPS) IPS Profiles page to manage IPS profiles. IPS profiles can be associated with IPS or exempt rules and deployed on a device by associating a profile with a firewall intent and deploying the firewall policy on the device.

Tasks You Can Perform

- Create an IPS profile—See [“Create IPS Profiles” on page 694](#).
- Edit, clone, or delete an IPS profile—See [“Edit, Clone, and Delete IPS Profiles” on page 695](#).
- Manage the IPS rules associated with an IPS profile—Click the **IPS-Profile-Name** to manage the IPS rules associated with the IPS profile. See [“About the <IPS-Profile-Name> / Rules Page” on page 697](#).
- Search for IPS profiles by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Sort IPS profiles—Click a column name to sort the data in the grid (table) based on the column name.

NOTE: Sorting is applicable only to some fields.

Field Descriptions

[Table 210 on page 693](#) describes the field on the IPS Profiles page.

Table 210: Fields on the IPS Profiles Page

Field	Description
Name	<p>Name of the IPS profile.</p> <p>Click the IPS-Profile-Name to manage the IPS rules associated with the IPS profile. The IPS-Profile-Name / Rules page appears. See “About the <IPS-Profile-Name> / Rules Page” on page 697.</p>
Definition Type	Indicates whether the IPS profile was system-generated (PREDEFINED) or created by a user (CUSTOM).
Description	Description of the IPS profile.

RELATED DOCUMENTATION

Create IPS Profiles

Contrail Service Orchestration (CSO) contains predefined intrusion prevention system (IPS) profiles that you can use. You can create customized IPS profiles from the Create IPS Profile page.

To create a customized IPS profile:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click the add (+) icon.

The Create IPS Profile page appears.

3. Complete the configuration according to the guidelines in [Table 211 on page 694](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the IPS Profiles page and a confirmation message is displayed indicating that the IPS profile is created.

After you create an IPS profile, you can add one or more IPS or exempt rules to the profile, and use the IPS profile in a firewall policy intent.

Table 211: Create IPS Profile Settings

Setting	Guideline
Name	Enter a unique name for the IPS profile that is a string of alphanumeric characters and some special characters (colon, hyphen, period, and underscore). No spaces are allowed and the maximum length is 255 characters.
Description	Enter a description for the IPS profile; the maximum length is 255 characters.

RELATED DOCUMENTATION

Create IPS or Exempt Rules | [699](#)

Adding Firewall Policy Intents | [449](#)

Edit, Clone, and Delete IPS Profiles

IN THIS SECTION

- [Edit IPS Profiles | 695](#)
- [Clone IPS Profiles | 696](#)
- [Delete IPS Profiles | 696](#)

You can edit, clone, or delete IPS profiles.

Edit IPS Profiles

You can edit only customized IPS profiles and not predefined (system-generated) profiles.

To edit a customized IPS profile:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Select a customized IPS profile and click the edit (pencil) icon.

The Edit IPS Profile page appears, displaying the same fields that are presented when you create an IPS profile.

3. Modify the IPS profile fields as needed. See [“Create IPS Profiles” on page 694](#).

NOTE: You can only modify the description and not the name.

4. Click **OK** to save your changes.

You are returned to the IPS Profiles page and a message that the IPS profile was successfully updated is displayed.

If the IPS profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone IPS Profiles

Cloning enables you to easily create a new IPS profile based on an existing one. You can clone predefined or customized IPS profiles and modify the parameters as needed.

To clone an IPS profile:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Select an IPS profile and select **More > Clone**.

The Clone IPS Profile page appears, displaying the same fields that are presented when you create an IPS profile.

3. Modify the IPS profile fields as needed. See [“Create IPS Profiles” on page 694](#).

4. Click **OK** to save your changes.

You are returned to the IPS Profiles page and a message that the IPS profile was successfully created is displayed.

Delete IPS Profiles

NOTE:

- You can delete only customized IPS profiles that are not referenced in a firewall policy intent.
- You cannot delete predefined (system-generated) IPS profiles.

To delete one or more customized IPS profiles:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Select one or more customized IPS profiles and click the delete (trash can) icon

A warning message appears asking you to confirm the deletion.

3. Click **Yes** to proceed with the deletion.

You are returned to the IPS Profiles page and a message indicating the status of the delete operation is displayed.

RELATED DOCUMENTATION

[About the <IPS-Profile-Name> / Rules Page | 697](#)

About the <IPS-Profile-Name> / Rules Page

IN THIS SECTION

- [Tasks You Can Perform | 697](#)
- [Field Descriptions | 698](#)

To access this page, select **Configure > IPS > IPS Profiles > *IPS-Profile-Name***.

Use the *IPS-Profile-Name* / Rules page to manage intrusion prevention system (IPS) rules and exempt rules. IPS profiles can be associated with IPS or exempt rules and deployed on a device by associating the IPS profile with a firewall policy intent and deploying the firewall policy on the device.

Tasks You Can Perform

- Create an IPS rule—See [“Create IPS or Exempt Rules” on page 699](#).
- Create an exempt rule—See [“Create IPS or Exempt Rules” on page 699](#).
- Edit, clone, or delete IPS or exempt rules—See [“Edit, Clone, and Delete IPS or Exempt Rules” on page 707](#).
- Search for rules by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Filter rules—Click the filter icon (funnel) and specify one or more filtering criteria. The filtered results are displayed on the same page.

NOTE: Filtering is applicable only to some fields.

Field Descriptions

Table 212 on page 698 describes the field on the *IPS-Profile-Name* / Rules page.

Table 212: Fields on the <IPS-Profile-Name> / Rules Page

Field	Description
Name	Name of the IPS rule or exempt rule.
IPS Signatures	Displays the IPS signatures associated with the IPS rule or exempt rule. If there is more than one signature associated with the rule, the number of additional signatures is displayed. Mouse over the number to view the full list of signatures.
IPS Action	<ul style="list-style-type: none"> For IPS rules, displays the action to be taken when the rule is matched. For exempt rules, displays Not Applicable because exempt rules are not associated with an action.
Additional Actions	<ul style="list-style-type: none"> For IPS rules, displays: <ul style="list-style-type: none"> Configured, if additional actions (to be taken when the rule is matched) are configured. Mouse over the gear icon to view the additional actions configured. Not Configured, if no additional actions are configured. For exempt rules, displays Not Applicable because exempt rules are not associated with any actions.
Details	<p>Displays whether the rule is an IPS rule or an exempt rule.</p> <p>Mouse over the Details field and then mouse over the ellipsis (...) displayed to access a menu to edit, clone, or delete the rule. See “Edit, Clone, and Delete IPS or Exempt Rules” on page 707.</p>

RELATED DOCUMENTATION

[About the IPS Signatures Page | 665](#)

[About the IPS Profiles Page | 692](#)

Create IPS or Exempt Rules

IN THIS SECTION

- [Create IPS Rules | 699](#)
- [Create Exempt Rules | 706](#)

You can create intrusion prevention system (IPS) rules or exempt rules only for customized IPS profiles.

Create IPS Rules

To create an IPS rule:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click ***IPS-Profile-Name*** for the profile for which you want to create a rule.

The *IPS-Profile-Name* / Rules page appears.

3. Select **Create > IPS Rule**.

The parameters for an IPS rule appear inline at the top of the page.

4. Complete the configuration according to the guidelines in [Table 213 on page 700](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

5. Click **Save** to save your changes.

The changes are saved and a confirmation message appears at the top of the page.

You can use the IPS profile in a firewall policy intent and deploy the firewall policy on the device, which deploys the IPS and exempt rules associated with the profile.

Table 213: Create IPS Rule Settings

Setting	Guideline
Rule Name	<p>CSO generates a unique rule name by default. You can modify the name if needed.</p> <p>The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.</p>
Description	Enter a description for the rule; the maximum length is 1024 characters.
IPS Signatures	<p>You can add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule:</p> <ol style="list-style-type: none"> Click inside the text box with the + icon. A list of IPS signatures and IPS signature static and dynamic groups appears. (Optional) Enter a search term and press Enter to filter the list of items displayed. Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule. (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups. Click the View more results link to view the full list of IPS signatures and IPS signature static and dynamic groups. The full list is displayed in the End Points panel on the right. To add one or more signatures, static groups, or dynamic groups: <ol style="list-style-type: none"> Mouse over a list item and select the check box that appears. Repeat the preceding step for the other signatures, static groups, or dynamic groups that you want to add. Click the check mark icon (✓) at the top of the End Points panel, and select Signatures. The signatures, static groups, or dynamic groups that you selected are added and displayed in the IPS Signatures field.

Table 213: Create IPS Rule Settings (continued)

Setting	Guideline
IPS Action	<p>Select the action to be taken when the monitored traffic matches the attack objects specified in the rules:</p> <ul style="list-style-type: none"> • None—No action is taken. Use this action to only generate logs for some traffic. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. • Close Client and Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Drop Connection—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address. • Recommended (default)—Uses the action that Juniper Networks recommends when that attack is detected. All predefined attack objects have a default action associated with them. • Diffserv Marking—Assigns the specified differentiated services code point (DSCP) value to the packet in an attack and pass the packet on normally. <p>When you select Diffserv Marking, you must enter a DSCP value:</p> <ol style="list-style-type: none"> 1. Click the Code Point: Vaule hyperlink. The Code point for Diffserve Marking action popup appears. 2. In the Code Point field, enter a DSCP value from 0 through 63. 3. Click OK. You are returned to the previous page; the value that you entered is displayed

Table 213: Create IPS Rule Settings (continued)

Setting	Guideline
Additional Actions	

Table 213: Create IPS Rule Settings (*continued*)

Setting	Guideline
	<p>In addition to the IPS action, you can configure one or more of the following additional actions:</p> <ul style="list-style-type: none"> Notifications—When attacks are detected, you can choose to log the attack and create log records with attack information and send that information to the log server. To configure notifications: <ol style="list-style-type: none"> Click the Notification link. The Notification page appears. Complete the configuration according to the guidelines shown in Table 214 on page 704. Click OK. You are returned to the previous page. A gear icon next to the Notification link indicates that you have configured notification settings. IP actions—When attacks are detected, you can configure actions that you want IPS to take against future connections that use the same IP address. To configure IP actions: <ol style="list-style-type: none"> Click the IP Action link. The IP Action page appears. Complete the configuration according to the guidelines shown in Table 215 on page 705. Click OK. You are returned to the previous page. A gear icon next to the IP Action link indicates that you have configured IP action settings. Additional actions—When attacks are detected, you can configure additional actions that you want CSO to take. To configure additional actions: <ol style="list-style-type: none"> Click the Additional link. The Additional page appears. Complete the configuration according to the guidelines shown in Table 216 on page 706. Click OK.

Table 213: Create IPS Rule Settings (*continued*)

Setting	Guideline
	You are returned to the previous page. A gear icon next to the Additional link indicates that you have configured additional settings.

Table 214: Notification Settings

Setting	Guideline
Attack Logging	Select the Enable check box to log an attack when it is detected.
Alert Flag	Select the Enable check box to set the alert flag in the attack log.
Log Packets	<p>Select the Enable check box to log packets when an attack is detected.</p> <p>In response to a rule match, you can capture the packets received before and after the attack for further offline analysis of attacker behavior. You can configure the number of pre-attack and post-attack packets to be captured for this attack, and limit the duration of post-attack packet capture by specifying a timeout value.</p> <p>You must specify at least one of the Packets Before, Packets After, or Post Window Timeout fields.</p>
Packets Before	<p>Specify the number of packets received before an attack that should be captured for further analysis of the behavior of the attack.</p> <p>Range: 1 through 255.</p>
Packets After	<p>Specify the number of packets received after an attack that should be captured for further analysis of attacker behavior.</p> <p>Range: 1 through 255.</p>
Post Window Timeout	<p>Specify a time limit (in seconds) for capturing packets received after an attack. No packets are captured after the specified timeout has elapsed.</p> <p>Range: 1 through 1800.</p>

Table 215: IP Action Settings

Setting	Guideline
IP Action	<p>Select the action to be taken on future connections that use the same IP address:</p> <p>NOTE: If there is an IP action match with more than one rule, then the most severe IP action of all the matched rules is applied. In decreasing order of severity, the actions are block, close, and notify.</p> <ul style="list-style-type: none"> • None (default)—Do not take any action. This is similar to if you did not configure the IP action. • IP Notify—Don't take any action on future traffic but log the event. • IP Close—Close future connections of new sessions that match the IP address by sending RST packets to the client and server. • IP Block—Block future connections of any session that matches the IP address.
IP Target	<p>Specify how the traffic should be matched for the configured IP actions:</p> <ul style="list-style-type: none"> • None—Do not match any traffic. • Destination Address—Match traffic based on the destination IP address of the attack traffic. • Service—For TCP and UDP, matches traffic based on the source IP address, source port, destination IP address, and destination port of the attack traffic. • Source Address—Matches traffic based on the source IP address of the attack traffic. • Source Zone—Matches traffic based on the source zone of the attack traffic. • Source Zone Address—Matches traffic based on the source zone and source IP address of the attack traffic. • Zone Service—Matches traffic based on the source zone, destination IP address, destination port, and protocol of the attack traffic.
Refresh Timeout	<p>Select the Enable check box to refresh the IP action timeout (that you specify in the Timeout Value field) if future traffic matches the IP actions configured.</p>
Timeout Value	<p>Configure the number of seconds that you want the IP action to remain in effect. For example, if you configure a timeout of 3600 seconds (1 hour) and traffic matches the IP actions configured, the IP action remains in effect for 1 hour.</p> <p>Range: 0 through 64,800 seconds.</p>
Log Taken	<p>Select the Enable check box to log the information about the IP action against the traffic that matches a rule.</p>
Log Creation	<p>Select the Enable check box generate an event when the IP action filter is triggered.</p>

Table 216: Additional Settings

Setting	Guideline
Severity	<p>Select a severity level to override the inherited attack severity in the rules.</p> <p>The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational is the least dangerous level and is used by network administrators to discover holes in their security systems.</p>
Terminal	Select the Enable check box to mark the IPS rule as terminal. When a terminal rule is matched, the device stops matching for the rest of the rules in that IPS profile.

Create Exempt Rules

To create an exempt rule:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click ***IPS-Profile-Name*** for the profile for which you want to create a rule.

The *IPS-Profile-Name* / Rules page appears.

3. Select **Create > Exempt Rule**.

The parameters for an exempt rule appear inline at the top of the page.

4. You can configure only the following fields:

- Rule Name
- Description
- IPS Signatures

See [Table 213 on page 700](#) for an explanation of these fields.

5. Click **Save** to save your changes.

The changes are saved and a confirmation message appears at the top of the page.

You can use the IPS profile in a firewall policy intent and deploy the firewall policy on the device, which deploy the IPS and exempt rules associated with the profile.

RELATED DOCUMENTATION

[Adding Firewall Policy Intents | 449](#)

Edit, Clone, and Delete IPS or Exempt Rules

IN THIS SECTION

- [Edit IPS or Exempt Rules | 707](#)
- [Clone IPS or Exempt Rules | 708](#)
- [Delete IPS or Exempt Rules | 708](#)

You can edit, clone, or delete IPS or exempt rules.

Edit IPS or Exempt Rules

You can edit IPS and exempt rules associated only with customized IPS profiles and not rules associated with predefined (system-generated) profiles.

To edit an IPS or an exempt rule:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click ***IPS-Profile-Name*** for the profile for which you want to edit a rule.

The *IPS-Profile-Name* / Rules page appears.

3. Mouse over the **Details** field, then mouse over the ellipsis (...) that appears, and from the menu, select **Edit**.

The rule that you selected for editing appears inline at the top of the page.

4. Modify the rule as needed. See [“Create IPS or Exempt Rules” on page 699](#).

NOTE: You can modify all fields except the name.

5. Click **Save** to save your changes.

The changes are saved and a confirmation message appears at the top of the page.

If the IPS or exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone IPS or Exempt Rules

Cloning enables you to easily create a new IPS or exempt rule based on an existing one. You can clone IPS and exempt rules associated only with customized IPS profiles and not rules associated with predefined (system-generated) profiles.

To clone an IPS or an exempt rule:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click **IPS-Profile-Name** for the profile for which you want to clone a rule.

The *IPS-Profile-Name / Rules* page appears.

3. Select a rule and select **More > Clone**. Alternatively, Mouse over the **Details** field, then mouse over the ellipsis (...) that appears, and from the menu, select **Clone**.

The rule that you selected for cloning appears inline at the top of the page.

4. Modify the rule as needed. See [“Create IPS or Exempt Rules” on page 699](#).

5. Click **Save** to save your changes.

The new rule is created and a confirmation message appears at the top of the page.

Delete IPS or Exempt Rules

You can delete IPS and exempt rules associated only with customized IPS profiles and not rules associated with predefined (system-generated) profiles.

To delete one or more IPS or exempt rules:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click ***IPS-Profile-Name*** for the profile for which you want to delete one or more rules.

The *IPS-Profile-Name* / Rules page appears.

3. Select one or more rules and click the delete (trash can) icon

A warning message appears asking you to confirm the deletion.

4. Click **Yes** to proceed with the deletion.

A message indicating the status of the delete operation appears at the top of the page.

If the IPS or exempt rule that you deleted belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

RELATED DOCUMENTATION

| [Adding Firewall Policy Intents](#) | 449

Managing SSL Proxies

IN THIS CHAPTER

- [SSL Forward Proxy Overview | 710](#)
- [About the SSL Proxy Policy Page | 716](#)
- [Creating SSL Proxy Policy Intents | 718](#)
- [Editing, Cloning, and Deleting SSL Proxy Policy Intents | 722](#)
- [Understanding How SSL Proxy Policy Intents Are Applied | 725](#)
- [About the SSL Proxy Profiles Page | 727](#)
- [Creating SSL Forward Proxy Profiles | 729](#)
- [Editing, Cloning, and Deleting SSL Forward Proxy Profiles | 733](#)
- [Configuring and Deploying an SSL Forward Proxy Policy | 736](#)

SSL Forward Proxy Overview

IN THIS SECTION

- [Supported Ciphers in Proxy Mode | 712](#)
- [Server Authentication | 713](#)
- [Root CA | 714](#)
- [Trusted CA List | 714](#)
- [Session Resumption | 715](#)
- [SSL Proxy Logs | 715](#)

Secure Sockets Layer (SSL) is an application-level protocol that provides encryption technology for the Internet. SSL, also called *Transport Layer Security* (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private–public key exchange pairs for this level of security.

Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a Web server. Confidentiality mechanisms ensure that communications are private. SSL enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on electronic communications. Finally, message integrity ensures that the contents of a communication have not been tampered with.

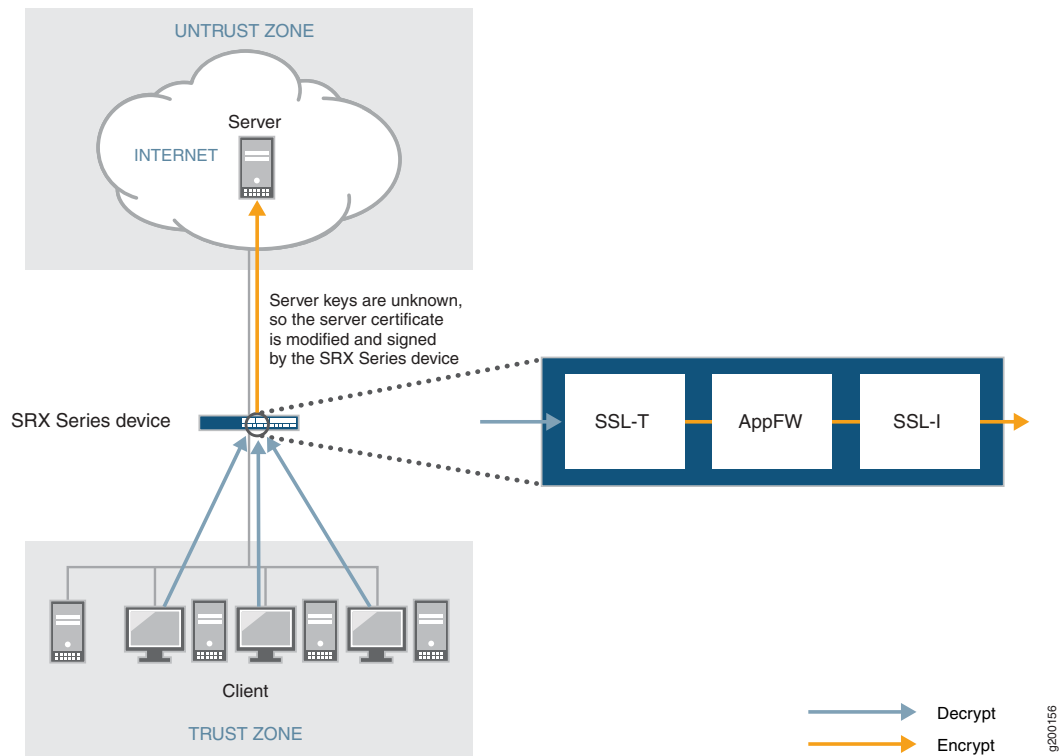
SSL forward proxy is a transparent proxy; that is, it performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL forward proxy ensures that it has the keys to encrypt and decrypt the payload:

- For the server, SSL forward proxy acts as a client—Because SSL forward proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.
- For the client, SSL forward proxy acts as a server—SSL forward proxy first authenticates the original server and replaces the public key in the original server certificate with a key that is known to it. It then generates a new certificate by replacing the original issuer of the certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL forward proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

[Figure 21 on page 712](#) shows how SSL forward proxy works on an encrypted payload. When application firewall (AppFW) is configured, SSL forward proxy acts as an SSL server terminating the SSL session from the client and a new SSL session is established to the server. The device decrypts and then re-encrypts all SSL forward proxy traffic. SSL forward proxy uses the following services:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.
- Configured AppFW services use the decrypted SSL sessions.

Figure 21: SSL Forward Proxy on an Encrypted Payload



This topic has the following sections:

Supported Ciphers in Proxy Mode

An SSL cipher comprises encryption ciphers, authentication method, and compression. [Table 217 on page 712](#) displays a list of supported ciphers. NULL ciphers are excluded.

The following SSL protocols are supported:

- SSLv3
- TLS1

Table 217: Supported Ciphers in Proxy Mode

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_MD5	RSA key exchange	128-bit RC4	Message Digest 5 (MD5) hash

Table 217: Supported Ciphers in Proxy Mode (*continued*)

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_SHA	RSA key exchange	128-bit RC4	Secure Hash Algorithm (SHA) hash
RSA_WITH_DES_CBC_SHA	RSA key exchange	DES CBC	SHA hash
RSA_WITH_3DES_EDE_CBC_SHA	RSA key exchange	3DES EDE/CBC	SHA hash
RSA_WITH_AES_128_CBC_SHA	RSA key exchange	128-bit AES/CBC	SHA hash
RSA_WITH_AES_256_CBC_SHA	RSA key exchange	256-bit AES/CBC	SHA hash
RSA_EXPORT_WITH_RC4_40_MD5	RSA-export	40-bit RC4	MD5 hash
RSA_EXPORT_WITH_DES40_CBC_SHA	RSA-export	40-bit DES/CBC	SHA hash
RSA_EXPORT1024_WITH_DES_CBC_SHA	RSA 1024 bit export	DES/CBC	SHA hash
RSA_EXPORT1024_WITH_RC4_56_MD5	RSA 1024 bit export	56-bit RC4	MD5 hash
RSA_EXPORT1024_WITH_RC4_56_SHA	RSA 1024 bit export	56-bit RC4	SHA hash
RSA-WITH-AES-256-GCM-SHA384	RSA key exchange	256-bit AES/GCM	SHA384 hash
RSA-WITH-AES-256-CBC-SHA256	RSA key exchange	256-bit AES/CBC	SHA256 hash
RSA-WITH-AES-128-GCM-SHA256	RSA key exchange	128-bit AES/GCM	SHA256 hash
RSA-WITH-AES-128-CBC-SHA256	RSA key exchange	128-bit AES/CBC	SHA256 hash

Server Authentication

Implicit trust between the client and the device (because the client accepts the certificate generated by the device) is an important aspect of SSL proxy. It is extremely important that server authentication is not compromised; however, in reality, self-signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.

You can specify that the SSL forward proxy should ignore server authentication completely. In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

You can specify whether the SSL proxy should ignore server authentication errors or not during the creation of an SSL forward proxy profile.

- If you specify that server authentication errors should *not* be ignored, the following scenarios occur:
 - If authentication succeeds, a new certificate is generated by replacing the keys and changing the issuer name to the issuer name that is configured in the root CA certificate in the proxy profile.
 - If authentication fails, the connection is dropped.
- If you specify that server authentication errors should be ignored, the following scenarios occur:

NOTE: We do not recommend that you configure this option for authentication because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.

- If the certificate is self-signed, a new certificate is generated by replacing the keys only. The issuer name is not changed. This ensures that the client browser displays a warning that the certificate is not valid.
- If the certificate has expired or if the common name does not match the domain name, a new certificate is generated by replacing the keys and changing the issuer name to SSL-PROXY: DUMMY_CERT:GENERATED DUE TO SRVR AUTH FAILURE. This ensures that the client browser displays a warning that the certificate is not valid.

Root CA

In a public key infrastructure (PKI) hierarchy, the root CA is at the top of the trust path. The root CA identifies the server certificate as a trusted certificate.

Trusted CA List

SSL forward proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL forward proxy checks certificate authority (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

Session Resumption

An SSL session refers to the set of parameters and encryption keys that are created when a full handshake is performed. A connection is the conversation or active data transfer that occurs within the session. The computational overhead of a complete SSL handshake and generation of master keys is considerable. In short-lived sessions, the time taken for the SSL handshake can be more than the time for data transfer. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a mechanism for caching sessions so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and the server. The cached information is identified by a session ID. In subsequent connections, both parties agree to use the session ID to retrieve the information rather than create a new pre-master secret key. Session resumption shortens the handshake process and accelerates SSL transactions.

SSL Proxy Logs

When logging is enabled in an SSL proxy profile, the SSL proxy can generate the messages shown in [Table 218 on page 715](#).

Table 218: SSL Proxy Logs

Log Type	Description
SSL_PROXY_SSL_SESSION_DROP	Logs generated when a session is dropped by SSL proxy.
SSL_PROXY_SSL_SESSION_ALLOW	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
SSL_PROXY_SESSION_IGNORE	Logs generated if non-SSL sessions are initially mistaken as SSL sessions.
SSL_PROXY_SESSION_WHITELIST	Logs generated when a session is allowed.
SSL_PROXY_ERROR	Logs used for reporting errors.
SSL_PROXY_WARNING	Logs used for reporting warnings.
SSL_PROXY_INFO	Logs used for reporting general information.

All logs contain similar information; the message field contains the reason for the log generation. One of three prefixes shown in [Table 219 on page 716](#) identifies the source of the message. Other fields are descriptively labeled.

Table 219: SSL Proxy Log Prefixes

Prefix	Description
system	Logs generated because of errors related to the device or an action taken as part of the SSL proxy profile. Most logs fall into this category.
openssl error	Logs generated during the handshake process if an error is detected by the openssl library.
certificate error	Logs generated during the handshake process if an error is detected in the certificate (X.509 related errors).

RELATED DOCUMENTATION

[About the SSL Proxy Policy Page | 716](#)
[About the SSL Proxy Profiles Page | 727](#)
[Certificates Overview | 416](#)

About the SSL Proxy Policy Page

To access this page, select **Configuration > SSL Proxy > Policy** in Customer Portal.

Use the SSL Proxy Policy page to view and manage SSL proxy policy intents. You can also deploy the SSL proxy policy immediately or schedule the deployment for later.

NOTE:

- When an SSL proxy intent is deployed, the corresponding certificates used in the SSL profile (associated with the SSL proxy intent) are automatically deployed to the applicable sites.
- If the application firewall (AppFW) service is not configured in the corresponding firewall policy intent, then the SSL forward proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy. Therefore, ensure that AppFW is configured for the firewall policy intents that should go through SSL inspection. If AppFW is not included in the policy intent, this does not cause an error; however, the SSL proxy action does not take place even though sessions are matched.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create SSL proxy policy intents—See [“Creating SSL Proxy Policy Intents” on page 718](#).
- Edit, clone, or delete SSL proxy policy intents—See [“Editing, Cloning, and Deleting SSL Proxy Policy Intents” on page 722](#).
- Search for SSL proxy policy intents by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Filter SSL proxy policy intents—Click the filter icon and select whether you want to show or hide column filters or apply a quick filter. Depending on your selection, you can filter the policy intents based on source, destination, or both, or view the filtered results. The filtered results are displayed on the same page.
- Deploy the SSL proxy policy—See [“Deploying Policies” on page 742](#).

Field Descriptions

[Table 220 on page 717](#) describes the fields on SSL Proxy Policy page.

Table 220: SSL Proxy Policy Page Fields

Field	Description
Total Intents	Total number of policy intents in the SSL proxy policy.
Undeployed	Number of SSL proxy policy intents that have not yet been deployed.
For each SSL proxy policy intent, the following information is displayed in a grid:	
Source	Source endpoints to which an SSL proxy policy intent applies.
Destination	Destination endpoints to which an SSL proxy policy intent applies..
SSL Proxy Profile	Name of the SSL proxy profile associated with the policy intent.
Options	Name and description of the SSL proxy policy intent.

RELATED DOCUMENTATION

Creating SSL Proxy Policy Intents

You can configure an SSL proxy policy intent inline on the SSL Proxy Policy page. An SSL proxy policy intent enables you to configure an SSL proxy between source and destination endpoints by associating the latter with an SSL proxy profile.

To create an SSL proxy policy intent:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The SSL Proxy Policy page appears.

2. Click the add icon (+).

The options to create policy intents appear inline on the SSL Proxy Policy page.

3. Enter the policy intent information according to the guidelines provided in [Table 221 on page 719](#)

4. Click **Save**.

The SSL proxy policy intent is saved and a confirmation message is displayed.

NOTE: After the policy intent is created, you must deploy the policy to ensure that the changes take effect on the applicable sites. When an SSL proxy policy intent is created, the **Undeployed** field is incremented by one indicating that intents are pending deployment.

Table 221: Create SSL Proxy Policy Intent Settings

Setting	Guideline
Source	<p>A source endpoint can be an IP address, an IP address group, a site, a site group, or a department, or or a combination of these.</p> <p>NOTE: A source IP address value of Any signifies any IP address from any site.</p> <p>Specify one or more source endpoints in one of the following ways:</p> <ul style="list-style-type: none"> • Click the add icon (+) and select the endpoints from the list of previously configured endpoints. • Filter the endpoints by entering a search term or one or more predefined keywords in the Source field and select one or more endpoints. <p>Table 222 on page 721 displays the list of predefined keywords.</p> <ul style="list-style-type: none"> • Click the View more results link to view additional configured endpoints. The list of endpoints is displayed in the End Points panel on the right. <p>Do one of the following:</p> <ul style="list-style-type: none"> • To add one endpoint at a time, select an endpoint and click the check mark icon (✓) that appears when you hover over the endpoint. • To add multiple endpoints, select one or more endpoints that you want to add, click the check mark icon (✓) at the top of the End Points panel, and select Source. • Filter the endpoints by entering a search term or one or more predefined keywords in the End Points field and select one or more endpoints. <p>Table 222 on page 721 displays the list of predefined keywords.</p> <p>NOTE: You can also create endpoints by clicking the add icon (+) in the End Points panel.</p> <p>Table 223 on page 722 displays the endpoints that can be created.</p>

Table 221: Create SSL Proxy Policy Intent Settings (*continued*)

Setting	Guideline
Destination	<p>A destination endpoint can be an IP address, an IP address group, a site, a site group, or a department, or or a combination of these.</p> <p>NOTE: A destination IP address value of Any signifies traffic going to the Internet (any address). Traffic within sites (internal traffic) is not covered by the destination IP address value of Any.</p> <p>If you want to cover traffic between two sites, ensure that the sites are included in both the source and destination endpoints.</p> <p>Specify one or more destination endpoints in one of the following ways:</p> <ul style="list-style-type: none"> • Click the add icon (+) and select the endpoints from the list of previously configured endpoints. • Filter the endpoints by entering a search term or one or more predefined keywords in the Destination field and select one or more endpoints. <p>Table 222 on page 721 displays the list of predefined keywords.</p> <ul style="list-style-type: none"> • Click the View more results link to view additional configured endpoints. The list of endpoints is displayed in the End Points panel on the right. <p>Do one of the following:</p> <ul style="list-style-type: none"> • To add one endpoint at a time, select an endpoint and click the check mark icon (✓) that appears when you hover over the endpoint. • To add multiple endpoints, select one or more endpoints that you want to add, click the check mark icon (✓) at the top of the End Points panel, and select Destination. • Filter the endpoints by entering a search term or one or more predefined keywords in the End Points field and select one or more endpoints. <p>Table 222 on page 721 displays the list of predefined keywords.</p> <p>NOTE: You can also create endpoints by clicking the add icon (+) in the End Points panel.</p> <p>Table 223 on page 722 displays the endpoints that can be created.</p>

Table 221: Create SSL Proxy Policy Intent Settings (*continued*)

Setting	Guideline
SSL Proxy Profile	<p>Specify an SSL proxy profile to associate with the SSL proxy policy intent in one of the following ways:</p> <ul style="list-style-type: none"> Click the add icon (+) and select the SSL proxy profile from the list of previously configured profiles. Filter the profiles by entering a search term in the SSL Proxy Profile field and select a profile. Create a SSL proxy profile—Click the Add New Profile link. The Create SSL Proxy Profiles page appears. See “Creating SSL Forward Proxy Profiles” on page 729. <p>NOTE: You can also create profiles by clicking the add icon (+) in the End Points panel and selecting SSL Proxy Profiles.</p> <ul style="list-style-type: none"> Click the View more results link to view additional configured profiles. The list of SSL proxy profiles is displayed in the End Points panel on the right. <p>To add a profile, select it and click the check mark icon (✓) that appears when you hover over the profile.</p>
Details	<p>Enter the name of the SSL proxy policy intent in the first text box. If you do not enter a name, the system-generated name is used. The name that you enter must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (- _). The maximum length is 63 characters.</p> <p>Enter the description of the SSL proxy policy intent in the second text box.</p>

Table 222: Keywords for Filtering Endpoints

Endpoint	Keyword	Applicable to
Address or Address Group	addr or ADDR	Source Destination
Site	site or SITE	Source Destination
Site Group	stgp or STGP	Source Destination
Department	dept or DEPT	Source Destination

Table 223: Creating Endpoints

Endpoint	Procedure
Address or Address Group	Click the add icon (+) and select Address . The Create Addresses page appears. See “Creating Addresses or Address Groups” on page 753 .
Site Group	Click the add icon (+) and select Site Group . The Create Site Group page appears. See “Creating Site Groups” on page 217 .
Department	Click the add icon (+) and select Department . The Create Department page appears. See “Add a Department” on page 783 .

RELATED DOCUMENTATION

| [SSL Forward Proxy Overview](#) | 710

Editing, Cloning, and Deleting SSL Proxy Policy Intents

IN THIS SECTION

- [Editing SSL Proxy Policy Intents](#) | 723
- [Cloning SSL Proxy Policy Intents](#) | 723
- [Deleting SSL Proxy Policy Intents](#) | 724

You can edit, clone, and delete SSL proxy policy intents from the SSL Proxy Policy page. This topic has the following sections:

Editing SSL Proxy Policy Intents

To modify the parameters configured for an SSL proxy policy intent:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The SSL Proxy Policy page appears, displaying the intents associated with the policy.

2. Hover over the SSL proxy policy intent that you want to edit, and then click the edit icon (pencil symbol) that appears on the right side of the intent.

You can now modify the policy intent inline on the SSL Proxy Policy page.

3. Modify the parameters following the guidelines provided in [“Creating SSL Proxy Policy Intents” on page 718](#).

4. Click **Save** to save your changes.

The SSL proxy policy intent is saved and a confirmation message is displayed.

NOTE: After a policy intent is modified, you must redeploy the policy to ensure that the changes take effect on the relevant sites. When an SSL proxy policy intent is modified, the **Undeployed** field is incremented by one indicating that intents are pending deployment.

Cloning SSL Proxy Policy Intents

Cloning enables you to easily create a new SSL proxy policy intent based on an existing one.

To clone an SSL proxy policy intent:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The **SSL Proxy Policy** page appears, displaying the intents associated with the policy.

2. Hover over the SSL proxy policy intent that you want to clone, and then click the clone icon that appears on the right side of the intent.

You can modify the cloned policy intent inline on the SSL Proxy Policy page.

3. Modify the parameters following the guidelines provided in [“Creating SSL Proxy Policy Intents” on page 718](#).

4. Click **Save** to save your changes.

The SSL proxy policy intent is cloned and a confirmation message is displayed.

NOTE: After a policy intent is cloned, you must redeploy the policy to ensure that the changes take effect on the relevant sites. When an SSL proxy policy intent is cloned, the **Undeployed** field is incremented by one indicating that one or more intents are pending deployment.

Deleting SSL Proxy Policy Intents

To delete one or more SSL proxy policy intents:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The **SSL Proxy Policy** page appears, displaying the intents associated with the policy.

2. Select the SSL proxy policy intents that you want to delete and then click the delete icon (X).

You are asked to confirm the delete operation.

3. Click **Yes** to delete the selected SSL proxy policy intents.

A confirmation message appears indicating the status of the delete operation.

NOTE: After one or more policy intents are deleted, you must redeploy the policy to ensure that the changes take effect on the applicable sites.

RELATED DOCUMENTATION

| [About the SSL Proxy Policy Page](#) | 716

Understanding How SSL Proxy Policy Intents Are Applied

IN THIS SECTION

- [Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match | 725](#)
- [Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match | 726](#)
- [Example 3: Applying SSL Proxy Policy Intents on Internal \(Site-to-Site\) Traffic | 726](#)

When you deploy an SSL proxy policy, SSL proxy profiles are deployed to the applicable sites based on SSL proxy policy intents. The deployments of firewall and SSL policies are related in that firewall policy deployments take into account the last-deployed SSL snapshots and vice versa. Therefore, even if an SSL proxy profile is deployed to the applicable sites, it is *applied* only to traffic to which the firewall policy intent applies.

The decision regarding *which* SSL proxy profile is attached to a firewall policy intent is based on matching criteria between SSL proxy policy and firewall policy intents. In addition, if there is a match between the SSL proxy policy intent and the firewall policy intent, the SSL profile is applied *only* to the policy intents that are common between the firewall and the SSL proxy policies.

The following examples demonstrate the matching logic between SSL proxy policy and firewall policy intents.

Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match

[Table 224 on page 725](#) shows an example of a firewall policy intent and an SSL proxy policy intent that match, which means that the SSL proxy profile attaches to the firewall policy intent. In this case, the firewall policy intent has a source and destination of **Any** IP address, which signifies traffic from any IP address from any site to any IP address on the Internet. The SSL proxy policy intent has a source of **Any** IP address, which signifies any IP address *from* any site, and a destination IP address of 198.51.100.0.

Therefore, there is a match between the firewall policy intent and the SSL proxy policy intent and the SSL proxy profile is applied *only* to traffic from any IP address of any site to the IP address 198.51.100.0.

Table 224: (Example) Match Between Firewall Policy Intent and SSL Proxy Policy Intent

Type	Source	Destination	Action or Profile
Firewall policy intent	IP address—Any	IP address—Any	Allow
SSL proxy policy intent	IP address—Any	IP address—198.51.100.0	SSL-Profile-1

Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match

Table 225 on page 726 shows an example of a firewall policy intent and an SSL proxy policy intent that do not match, which means that the SSL proxy profiles do not attach.

Although, at first glance, it *appears* that an SSL proxy policy intent with a source and destination IP address **Any** should match a firewall policy intent with a source IP address **Any** and destination department Finance, this is not the case because of what the IP address **Any** signifies in the destination.

For both firewall and SSL proxy policy intents:

- A source IP address value of **Any** signifies any IP address *from* any site.
- A destination IP address value of **Any** signifies traffic going *to* the Internet—that is, to any IP address on the Internet. Traffic *within* sites (internal traffic) is not covered by the destination IP address value of **Any**.

In this example, the firewall policy intent applies to traffic from any IP address (from any site) to the Finance department. However, the SSL proxy policy intent applies to traffic from any IP address (from any site) to any IP address on the Internet. This means that there is no match between the firewall policy intent and the SSL proxy policy intent and the SSL proxy profile does not attach.

Table 225: (Example) No Match Between Firewall Policy Intent and SSL Proxy Policy Intent

Type	Source	Destination	Action or Profile
Firewall policy intent	IP address—Any	Department—Finance	Allow
SSL proxy policy intent	IP address—Any	IP address—Any	SSL-Profile-2

Example 3: Applying SSL Proxy Policy Intents on Internal (Site-to-Site) Traffic

NOTE: SSL forward proxy typically might not be used for site-to-site traffic, but this example is provided as an explanation of how an SSL proxy policy intent applies to site-to-site traffic.

Consider a scenario in which you have three sites (A, B, C) and you want to configure an SSL proxy for traffic between the sites. Table 226 on page 727 displays the firewall policy and SSL proxy policy intents that you can use for such a scenario.

Both the firewall policy intent and the SSL proxy policy intent use Site A, Site B, and Site C as the source and destination. Therefore, the firewall policy intent and the SSL proxy policy intent match, and the SSL proxy profile attaches to the firewall policy intent.

NOTE: The destination must be Site A, Site B, and Site C because the destination IP address **Any** signifies any IP address on the *Internet*.

Table 226: (Example) Firewall Policy and SSL Proxy Policy Intents for Site-to-Site Traffic

Type	Source	Destination	Action or Profile
Firewall Policy Intent	Site A, Site B, Site C	Site A, Site B, Site C	Allow
SSL Proxy Policy Intent	Site A, Site B, Site C	Site A, Site B, Site C	SSL-Profile-3

RELATED DOCUMENTATION

[SSL Forward Proxy Overview | 710](#)

[Configuring and Deploying an SSL Forward Proxy Policy | 736](#)

About the SSL Proxy Profiles Page

To access this page, click **Configuration > SSL Proxy > Profiles** in Customer Portal.

Use the SSL Proxy Profiles page to view and manage SSL proxy profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an SSL proxy profile—See [“Creating SSL Forward Proxy Profiles” on page 729](#).
- Edit, clone, or delete an SSL proxy profile—See [“Editing, Cloning, and Deleting SSL Forward Proxy Profiles” on page 733](#).
- View the details of an SSL proxy profile—Select the SSL proxy profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The View SSL Proxy Profile Details page appears. [Table 228 on page 728](#) describes the fields on this page.
- Search for SSL proxy profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Widget Descriptions

Table 227 on page 728 describes the fields on the SSL Proxy Profiles page.

Table 227: Fields on the SSL Proxy Profiles Page

Field	Description
Name	Name of the SSL proxy profile.
Preferred Cipher	Preferred cipher associated with the profile.
Custom Ciphers	The set of ciphers, if the preferred cipher is Custom , which the SSH server uses to perform encryption and decryption functions.
Exempted Address	Addresses that can are exempted from SSL forward proxy processing.
Description	Description of the SSL proxy profile.
Root Certificate	Root certificate associated with the SSL proxy profile.

Table 228: View SSL Forward Proxy Profile Details Page Fields

Field	Description
General Information	
Name	Name of the SSL proxy profile.
Description	Description of the SSL proxy profile.
Preferred Cipher	Preferred cipher associated with the proxy profile.
Custom Ciphers	The set of ciphers, if the preferred cipher is Custom , which the SSH server uses to perform encryption and decryption functions.
Flow Trace Enabled	Indicates whether flow tracing is enabled or disabled.
Certificates	Displays the root certificate and the trusted certificate authorities associated with the root certificate.
Exempted Address	Addresses that can are exempted from SSL forward proxy processing.
Exempted URL Categories	URL categories that are exempted from SSL forward proxy processing.
Actions	

Table 228: View SSL Forward Proxy Profile Details Page Fields (*continued*)

Field	Description
Ignore	Indicates whether server authentication failure is ignored (Enabled) or not (Disabled).
Session Resumption	Indicates whether session information is cached to enable session resumption (Enabled) or not (Disabled).
Logging	If logging is enabled, indicates the type of events that are logged.
Renegotiation	Indicates the type of renegotiation required if there is a change in SSL parameters after a session is created and SSL tunnel transport is established.

RELATED DOCUMENTATION

[About the SSL Proxy Policy Page](#) | 716

Creating SSL Forward Proxy Profiles

Use this page to configure SSL forward proxy profiles. SSL proxy is enabled as an application service within a security policy. You specify the traffic that you want the SSL proxy enabled on as match criteria and then specify the SSL proxy profile to be applied to the traffic.

To create an SSL forward proxy profile:

NOTE: Ensure that you have a root certificate imported for the tenant before you create an SSL forward proxy profile. You can import SSL certificates (root and trusted) from the Certificates page (**Administration > Certificates**) and associate the certificates with SSL forward proxy profiles.

1. Select **Configuration > SSL Proxy > Profiles** in Customer Portal.

The SSL Proxy Profiles page appears.

2. Click the add icon (+) to create an SSL forward proxy profile.

The Create SSL Proxy Profiles page appears.

3. Complete the configuration according to the guidelines provided in [Table 229 on page 730](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

An SSL forward proxy profile is created. You are returned to the SSL Proxy Profiles page where a confirmation message is displayed.

The SSL forward proxy profile can be used in an SSL proxy policy intent (**Configuration > SSL Proxy > Policy**).

Table 229: Creating SSL Forward Proxy Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the profile, which is string of alphanumeric characters and some special characters (- _). No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the profile. The maximum length is 255 characters.
Preferred Cipher	Select a preferred cipher. Preferred ciphers enable you to define an SSL cipher that can be used with acceptable key strength. You can select from the following categories: <ul style="list-style-type: none">• None (Default)—Do not specify a preferred cipher.• Medium—Use ciphers with key strength of 128 bits or greater.• Strong—Use ciphers with key strength of 168 bits or greater.• Weak—Use ciphers with key strength of 40 bits or greater.• Custom—Configure a custom cipher suite.

Table 229: Creating SSL Forward Proxy Profile Settings (*continued*)

Setting	Guideline
Custom Ciphers	<p>If you specified Custom as the preferred cipher, you can define a custom cipher list by selecting ciphers.</p> <p>Select the set of ciphers that the SSH server can use to perform encryption and decryption functions.</p> <p>The available custom ciphers are:</p> <ul style="list-style-type: none"> • <code>rsa-with-RC4-128-md5</code>—RSA, 128-bit RC4, MD5 hash • <code>rsa-with-RC4-128-sha</code>—RSA, 128-bit RC4, SHA hash • <code>rsa-with-des-cbc-sha</code>—RSA, DES/CBC, SHA hash • <code>rsa-with-3DES-ede-cbc-sha</code>—RSA, 3DES EDE/CBC, SHA hash • <code>rsa-with-aes-128-cbc-sha</code>—RSA, 128-bit AES/CBC, SHA hash • <code>rsa-with-aes-256-cbc-sha</code>—RSA, 256 bit AES/CBC, SHA hash • <code>rsa-export-with-rc4-40-md5</code>—RSA-export, 40 bit RC4, MD5 hash • <code>rsa-export-with-des40-cbc-sha</code>—RSA-export, 40 bit DES/CBC, SHA hash • <code>rsa-export1024-with-des-cbc-sha</code>—RSA 1024 bit export, DES/CBC, SHA hash • <code>rsa-export1024-with-rc4-56-md5</code>—RSA 1024 bit export, 56 bit RC4, MD5 hash • <code>rsa-export1024-with-rc4-56-sha</code>—RSA 1024 bit export, 56 bit RC4, SHA hash • <code>rsa-with-aes-256-gcm-sha384</code>—RSA, 256 bit AES/GCM, SHA384 hash • <code>rsa-with-aes-256-cbc-sha256</code>—RSA, 256 bit AES/CBC, SHA256 hash • <code>rsa-with-aes-128-gcm-sha256</code>—RSA, 128 bit AES/GCM, SHA256 hash • <code>rsa-with-aes-128-cbc-sha256</code>—RSA, 256 bit AES/CBC, SHA256 hash • <code>ecdhe-rsa-with-aes-256-gcm-sha384</code>—ECDHE, RSA, 256 bit AES/GCM, SHA384 hash • <code>ecdhe-rsa-with-aes-256-cbc-sha384</code>—ECDHE, RSA, 256 bit AES/CBC, SHA384 hash • <code>ecdhe-rsa-with-aes-256-cbc-sha</code>—ECDHE, RSA, 256 bit AES/CBC, SHA hash • <code>ecdhe-rsa-with-aes-3des-ede-cbc-sha</code>—ECDHE, RSA, 3DES, EDE/CBC, SHA hash • <code>ecdhe-rsa-with-aes-128-gcm-sha256</code>—ECDHE, RSA, 128 bit AES/GCM, SHA256 hash • <code>ecdhe-rsa-with-aes-128-cbc-sha256</code>—ECDHE, RSA, 128 bit AES/CBC, SHA256 hash • <code>ecdhe-rsa-with-aes-128-cbc-sha</code>—ECDHE, RSA, 128 bit AES/CBC, SHA hash
Flow Trace	Select this option to enable flow tracing to enable the troubleshooting of policy-related issues.
Root Certificate	Select or add a root certificate. In a public key infrastructure (PKI) hierarchy, the root certificate authority (CA) is at the top of the trust path.

Table 229: Creating SSL Forward Proxy Profile Settings (*continued*)

Setting	Guideline
Trusted Certificate Authorities	<p>Choose whether you want to add all trusted certificates present on the device (All) or select specific trusted certificates. Before establishing a secure connection, the SSL proxy checks CA certificates to verify signatures on server certificates.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Specifying that all trusted certificates should be used means that all trusted certificates on a particular device (site) will be used during SSL policy deployment. • If you specify that all trusted certificates should be used in an SSL forward proxy profile, you must ensure that at least one trusted certificate is installed on the device.
Actions	
Exempted Addresses	<p>Exempted addresses include addresses that you want to exempt from undergoing SSL proxy processing.</p> <p>To specify exempted addressees, select one or more addresses in the Available column and click the forward arrow to confirm your selection. The selected addresses are then displayed in the Selected column. These addresses are used to create allowlists that bypass SSL forward proxy processing.</p> <p>Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass SSL proxy processing for some sessions.</p> <p>Such sessions typically include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under allowlists.</p> <p>NOTE: You can also add addresses by clicking Add New Address. The Create Addresses page appears. See “Creating Addresses or Address Groups” on page 753.</p>
Exempted URL Categories	Select the previously defined URL categories to create allowlists that bypass SSL forward proxy processing. The selected URL categories are exempted during SSL inspection.
Server Auth Failure	<p>Select this check box to ignore errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry). This check box is cleared by default.</p> <p>We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.</p>

Table 229: Creating SSL Forward Proxy Profile Settings (*continued*)

Setting	Guideline
Session Resumption	<p>Select this check box to disable session resumption. This check box is cleared by default.</p> <p>To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a session-caching mechanism so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and server.</p>
Logging	<p>Select one or more events to be logged. You can choose to log all events, warnings, general information, errors, or different sessions (allowed, dropped, or ignored). Logging is disabled by default.</p>
Renegotiation	<p>Select one of the following options if a change in SSL parameters requires renegotiation:</p> <ul style="list-style-type: none"> • None (default)—Indicates that renegotiation is not required. • Allow—Allow secure and nonsecure renegotiation. • Allow-secure—Allow secure negotiation only. • Drop—Drop session on renegotiation request. <p>After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. SSL forward proxy supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) renegotiation.</p> <p>When session resumption is enabled, session renegotiation is useful in the following situations:</p> <ul style="list-style-type: none"> • Cipher keys need to be refreshed after a prolonged SSL session. • Stronger ciphers need to be applied for a more secure connection.

RELATED DOCUMENTATION

[About the SSL Proxy Policy Page](#) | 716

Editing, Cloning, and Deleting SSL Forward Proxy Profiles

IN THIS SECTION

- [Editing SSL Forward Proxy Profiles](#) | 734
- [Cloning SSL Forward Proxy Profiles](#) | 734
- [Deleting SSL Forward Proxy Profiles](#) | 735

You can edit, clone, and delete SSL forward proxy profiles from the SSL Proxy Profiles page. This topic has the following sections:

Editing SSL Forward Proxy Profiles

To modify the parameters configured for an SSL forward proxy profile:

NOTE: If an SSL forward proxy profile is already used in an SSL proxy policy intent, we recommend that you do not modify the profile name. If you want to create a profile with a new name, clone the existing profile and modify the name.

1. Select **Configuration > SSL Proxy > Profiles**.

The SSL Proxy Profiles page appears, displaying the existing SSL forward proxy profiles.

2. Select the SSL forward proxy profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.

The Edit SSL Proxy Profile page appears showing the same fields that are presented when you create an SSL forward proxy profile.

3. Modify the SSL forward proxy profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the SSL Proxy Profiles page. A confirmation message appears, indicating the status of the edit operation.

NOTE: If an SSL forward proxy profile that is associated with an SSL proxy policy intent is modified, you must redeploy the SSL proxy policy to ensure that the changes take effect on the site.

Cloning SSL Forward Proxy Profiles

Cloning enables you to easily create a new SSL forward proxy profile based on an existing one.

To clone an SSL forward proxy profile:

1. Select **Configuration > SSL Proxy > Profiles**.

The SSL Proxy Profiles page appears displaying the existing SSL forward proxy profiles.

2. Select the SSL forward proxy profile that you want to clone and select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone SSL Proxy Profile page appears, showing the same fields that are presented when you create an SSL forward proxy profile.

3. Modify the SSL forward proxy profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the SSL Proxy Profiles page. A confirmation message appears, indicating the status of the clone operation.

Deleting SSL Forward Proxy Profiles

To delete one or more SSL forward proxy profiles:

NOTE: If you try to delete an SSL forward proxy profile that is associated with an SSL proxy policy intent, a message is displayed indicating that the profile cannot be deleted.

1. Select **Configuration > SSL Proxy > Profiles**.

The SSL Proxy Profiles page appears, displaying the existing SSL forward proxy profiles.

2. Select one or more SSL forward proxy profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete SSL Proxy Profile**.

An alert message appears asking you to confirm the delete operation.

3. Click **Yes** to delete the selected SSL forward proxy profiles.

A confirmation message appears indicating the status of the delete operation.

NOTE: If the deleted SSL forward proxy profile is associated with an SSL proxy policy intent, you must redeploy the SSL proxy policy to ensure that the changes take effect on the site.

RELATED DOCUMENTATION

[Creating SSL Forward Proxy Profiles | 729](#)[About the SSL Proxy Profiles Page | 727](#)

Configuring and Deploying an SSL Forward Proxy Policy

The following is the workflow for configuring and deploying an intent-based SSL forward proxy policy in CSO:

1. Obtain the root certificate and private key from your trusted certificate authority (CA).
2. Combine the root certificate and private key into a single file.
3. Import the certificate and private key file (on the Import Certificate page); see [“Importing a Certificate” on page 419](#).
4. (Optional) Install the imported certificate on one or more sites (on the Install Certificate page); see [“Installing and Uninstalling Certificates” on page 421](#).
5. By default, Juniper Networks ships trusted certificates for sites that use HTTPS. These certificates are installed automatically by CSO when the site is successfully provisioned.

If you want to use additional trusted certificates, import and install the certificates as explained in [Step 3](#) and [4](#).

6. Create an SSL proxy profile (on the Create SSL Proxy Profiles) page; see [“Creating SSL Forward Proxy Profiles” on page 729](#).

NOTE:

- Use the imported root certificate when you create the SSL proxy profile.
- For trusted certificates, specify that all trusted certificates on the device are used (select **All** in the **Trusted Certificate Authorities** field).

7. Create an SSL proxy policy intent that uses the SSL proxy profile that you created (on the SSL Proxy Policy page); see [“Creating SSL Proxy Policy Intents” on page 718](#).
8. Deploy the SSL proxy policy; see [“Deploying Policies” on page 742](#).

NOTE:

- Ensure that the root and trusted certificates are imported into CSO before the policy is deployed.
- If you have not installed the certificates referenced in the SSL proxy profile, then they are automatically installed when the SSL proxy policy is deployed.

9. For Internet access from an SRX Series device by using the SSL proxy, ensure that you import the root certificate (obtained in Step 1) into the browsers of the clients accessing the Internet.

NOTE: If you do not import the certificate, the traffic does not go through for clients in the LAN segments.

RELATED DOCUMENTATION

[SSL Forward Proxy Overview | 710](#)

[Understanding How SSL Proxy Policy Intents Are Applied | 725](#)

Deploying Policies

IN THIS CHAPTER

- [Deploying Policies Overview | 738](#)
- [About the Deployments Page | 739](#)
- [Using the Deployment Icon to Deploy Policies | 741](#)
- [Deploying Policies | 742](#)

Deploying Policies Overview

When you finish creating and verifying your security configurations, you can deploy these configurations and keep them ready to be pushed to the security devices. CSO enables you to push security configurations to the devices all at once by providing a single interface that is intuitive.

The deployment workflow provides the ability to save and publish different services to be updated at a later time to the appropriate firewalls (during downtime). This enables administrators to review their firewall and NAT policies before updating the device. Administrators also save troubleshooting time, avoid errors, and save costs associated with errors. Verify and tweak your security configurations before updating them to the device. This approach helps you keep the configurations ready and update these configurations to the devices during the maintenance window.

When you deploy policies, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such dependent policies do not need to be republished in order for their changes in priority or precedence to take effect. It will be enough if the policy which is updated is republished.

There are three ways in which you can view and deploy your security configurations:

- Click on the deployment icon present in the CSO Customer Portal banner and use the deployment panel that appears, to deploy policies. See [“Using the Deployment Icon to Deploy Policies” on page 741](#).

NOTE: The deployment icon is highlighted in orange if there are undeployed configurations.

- Use the **Deployments** page. See [“About the Deployments Page” on page 739](#).
- Select a firewall, NAT or SD-WAN policy from its respective landing pages and click **Deploy**. For more information, see [“Deploying Policies” on page 742](#).

RELATED DOCUMENTATION

[Using the Deployment Icon to Deploy Policies | 741](#)

[About the Deployments Page | 739](#)

[Deploying Policies | 742](#)

About the Deployments Page

To access this page, click **Configuration > Deployments**.

Use this page to deploy or schedule the deployment of undeployed SD-WAN, NAT, and firewall policies. Undeployed policies refer to newly created firewall policy rules or NAT policies. These changes do not come into effect until the policies are deployed. The **Deploy** page provides scheduling options for you to deploy these policies.

Tasks You Can Perform

You can perform the following task from this page:

- Deploy a policy. See [“Deploying Policies” on page 742](#).

Field Descriptions

[Table 230 on page 740](#) provides guidelines on using the fields on the **Deployments** page.

Table 230: Fields on the Deployments Page

Field	Description
Awaiting Deployment	<p>The Awaiting Deployment tab displays all the policies that are awaiting deployment. The following fields provide more information about the undeployed policies:</p> <ul style="list-style-type: none"> • Name—Name of the policy that needs to be deployed. • Deployment Type—Type of the policy that needs to be deployed. • Summary—Description of the policy. • Owner—The tenant who has created the policy. • Last updated—The last time the policy was updated. <p>If you want to deploy a policy, select the policy and click Deploy. The policy is deployed and will no longer appear in the Awaiting Deployment tab.</p> <p>If you want to refresh the Awaiting Deployment tab, click the refresh icon provided below the details table.</p>
Scheduled	<p>The Scheduled tab displays all the policies that have been scheduled for deployment on a certain date and time. The following fields provide more information about scheduled policies:</p> <ul style="list-style-type: none"> • Name—Name of the policy. • Deployment Type—Type of the policy that needs to be deployed. • Summary—Description of the policy. • Schedule—The date and time at which the policy is scheduled to be deployed. • Status—Displays whether the scheduled policy has been deployed or not. • Next Run—Date and time when the scheduled deployments will be run. <p>If you want to deploy a scheduled policy immediately, select the policy and click Deploy Now. If you want to modify the deployment schedule of a policy, select the policy and click the edit icon (pencil icon). The Deploy page appears displaying the current scheduling information. See “Deploying Policies” on page 742, to update the schedule.</p>
History	<p>The History tab displays all the policies that have been deployed. The following fields provide more information about deployed policies:</p> <ul style="list-style-type: none"> • Name—Name of the deployed policy. • Deployment Type—Type of the deployed policy. • Summary—Description of the policy. • Status—Displays the status of the deployed policy. • Job Details—Details of the job. • Deployed On—Date and time the policy was deployed. <p>If you want to redeploy a policy, select the policy and click Re-Deploy. The policy is redeployed and the History tab details changes to reflect this information.</p>

RELATED DOCUMENTATION

Deploying Policies Overview 738
Using the Deployment Icon to Deploy Policies 741
Deploying Policies 742

Using the Deployment Icon to Deploy Policies

CSO provides an option of viewing and deploying policies through the deployment panel, that appears when you click on the deployment icon. The deployment icon is highlighted in orange if there are undeployed policies.

To deploy policies through the deployment panel:

1. Click the deployment icon on the Customer Portal banner.
The deployment panel appears. For information about the panel, see [Table 231 on page 741](#).
2. Hover over the policy you want to deploy. The **Deploy** option appears on the right side of the policy.
3. Click **Deploy** to deploy the policy. For more information, see [“Deploying Policies” on page 742](#).

[Table 231 on page 741](#) provides guidelines on using the fields on the deployment panel.

Table 231: Fields on the Deployment Panel

Field	Description
Awaiting Deployment	The Awaiting Deployment tab displays all the policies that are awaiting deployment.
In Progress	The In Progress tab displays all the policies that are currently being deployed.

RELATED DOCUMENTATION

Deploying Policies Overview 738
About the Deployments Page 739
Deploying Policies 742

Deploying Policies

You can deploy firewall, NAT, SD-WAN, and SSL proxy policies added by various services immediately or schedule the deployment for a later date and time.

To configure a deployment:

1. You can initiate the deployment of a policy in the following ways:
 - Select a policy from the **Awaiting Deployment** tab on the **Deployments** page and click **Deploy**.
 - Select a policy from the **Scheduled** tab on the **Deployments** page and click **Deploy**.
 - Select a policy from the **Scheduled** tab on the **History** page and click **Re-Deploy**.
 - Use the deployment icon on the Customer Portal banner. For more information about deploying policies using the deployment icon, see [“Using the Deployment Icon to Deploy Policies” on page 741](#).

NOTE: The deployment icon is highlighted in orange if there are undeployed policies.

- Select **Configuration > Firewall > Firewall Policy**. The **Firewall Policy** page appears, displaying the intents associated with the policy. Click **Deploy**.
 - Select **Configuration > NAT > NAT Policies** and select the NAT policy you want to deploy. Click **Deploy**.
 - Select **Configuration > SSL Proxy > Policy**. The **SSL Proxy Policy** page appears, displaying the intents associated with the policy. Click **Deploy**.
 - Select an SD-WAN policy intent on the **SD-WAN Policy** page and click **Deploy**.
2. The **Deploy** page appears. In **Choose Deployment Time** options, select **Run Now** to deploy the policy immediately.

Select **Schedule at a later time** to deploy the policy at a later date and time. For scheduling options, see [Table 232 on page 742](#).

3. Click **Deploy**.

[Table 232 on page 742](#) provides guidelines on using the fields on the **Deploy** page.

Table 232: Fields on the Deploy Page

Field	Description
Summary	
Policies	The summary of the policy that is to be deployed.

Table 232: Fields on the Deploy Page *(continued)*

Field	Description
Choose Deployment Time	
Type	<ul style="list-style-type: none">• Select Run now if you want to deploy the policy immediately.• Select Schedule at a later time if you want to schedule the deployment for a later date and time.<ul style="list-style-type: none">• Click on the calendar icon to choose the date for the deployment in MM/DD/YYYY format.• Enter the time for the deployment in HH:MM:SS format. You can choose the 12 hour (AM or PM) or 24 hour format to specify the time by selecting the option from the drop-down list provided beside the time field.

NOTE: If a tenant with the SD-WAN Advanced service selects an SLA or cloud-based profile for both SD-WAN Essentials and Advanced sites, the SD-WAN deploy job fails indicating the intents that failed for the SD-WAN Essentials sites. The intents are added to the SD-WAN Advanced sites.

RELATED DOCUMENTATION

Deploying Policies Overview 738
Using the Deployment Icon to Deploy Policies 741
About the Deployments Page 739

5

PART

Managing Network Services and Shared Objects

Configuring Network Services | **745**

Managing Shared Objects | **750**

Configuring Network Services

IN THIS CHAPTER

- [Network Service Overview | 745](#)
- [About the Network Services Page | 746](#)
- [About the Service Instances Page | 748](#)

Network Service Overview

A *network service* is a final product offered to end users with a full description of its functionality and specified performance.

Administrative users deploy network services between two locations in a virtual network, so that traffic traveling in a specific direction on that link is subject to action from that service. The term *network service* is defined in the ETSI Network Functions Virtualization (NFV) standard.

A network service consists of a *service chain* of one or more linked network functions, which are provided by specific virtualized network functions (VNFs), with a defined direction for traffic flow and defined ingress and egress points. The term service chain refers to the structure of a network service, and although not defined in the ETSI NFV standard, this term is regularly used in NFV and software-defined networking (SDN).

A network service designer creates network services in Network Service Designer. When the designer publishes the service to the network service catalog from Network Service Designer, administrators can see the network service in Administration Portal.

RELATED DOCUMENTATION

[About the Network Services Page | 746](#)

About the Network Services Page

To access this page, click **Configuration > Network Services**.

You can use the Network Services page to view the complete list of network services that service designers have published to the network service catalog from network service designer and to view information about the services. For an introduction to network services, see [“Network Service Overview” on page 745](#).

Tasks You Can Perform

You can perform the following tasks from this page:

- Quickly view important data about network services and about instances of those services deployed at customers’ sites in the widgets that appear at the top of the page. See [Table 233 on page 746](#).
- View full information about a service and about instances of a service at customer sites. Click the name of a service in the list. See [“About the Service Instances Page” on page 748](#).

Field Descriptions

[Table 233 on page 746](#) shows the descriptions of the widgets that appear at the top of the Network Services page.

Table 233: Widgets on the Network Services Page

Widget	Description
Top Network Services Instantiated	<p>View the numbers of instances of the three services that are most used by tenants in the network.</p> <p>This view helps you identify trends for network services, especially when you introduce a new service.</p>
Services with Critical Alerts	View the top three network services receiving the maximum number of critical alerts.
Top Services by POP CPU Usage	View the top three network services using the largest percentage of CPU from the assigned CPU cores.

[Table 234 on page 747](#) shows the descriptions of the fields on the Network Services page.

Table 234: Fields on the Network Services Page

Field	Description
Name	View the name of the service. Click the name to view full information about a service.
Tenants	View the names of the tenants that have access to the network service.
Sites	View the total number of sites at which the service is deployed for the tenant. Example: 2
Instances	View the total number of occurrences of the service that administrative users have activated for the tenant. Example: 1
Last Update	View the date on which the network service designer last modified the service.

[Table 235 on page 747](#) shows the descriptions of the fields on the Detail for *network service name* page.

Table 235: Fields on the Network Service Detail Page

Field	Description
<i>General</i>	
Configuration	View the settings that the network service designer or you have configured for this service.
Version	View the version number of the network service. Example: 1.1
State	View the status of the network service. Example: Published
Performance Goals	View performance parameters of the network service that include bandwidth, number of sessions, latency, and license cost.

RELATED DOCUMENTATION

[Network Service Overview](#) | 745

About the Service Instances Page

To access this page, click **Services** > *Service Name* > **Instances**

You can use the Service Instances page to view information about occurrences of the service at specific customer sites.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a service instance. Click the details icon that appears when you hover over the name of a service. See [Table 237 on page 749](#).
- Enable or disable a network service or virtualized network function (VNF) recovery. Select a service instance and click **Enable Auto Healing** to enable automatic recovery of a network service or VNF.

Field Descriptions

[Table 236 on page 748](#) shows the descriptions of the fields on the Service Instances page.

Table 236: Fields on the Service Instances Page

Field	Description
Name	View the name of the occurrence of a service at a specific tenant site.
Tenant	View the name of the tenant.
Status	View the state of the service at the customer site: <ul style="list-style-type: none"> • Created—Administrative user for the tenant has enabled this service instance, which is active. • Blank—Administrative user for the tenant has disabled this service instance.
Site	View the name of the site at which service occurrence is available.
POP	View the POP in which the site is located.
Functions	View network functions that the service offers; for example, Network Address Translation (NAT) or firewall.

[Table 237 on page 749](#) shows the descriptions of the fields on the Detail for *Service-Instance-Name* page.

Table 237: Fields on the Service Instance Details Page

Field	Description
<i>General</i>	
Description	View information about this service instance. This information is generated from data in Customer Portal.

RELATED DOCUMENTATION

Network Service Overview 745
About the Network Services Page 746

Managing Shared Objects

IN THIS CHAPTER

- [Addresses and Address Groups Overview | 751](#)
- [About the Addresses Page | 751](#)
- [Creating Addresses or Address Groups | 753](#)
- [Editing, Cloning, and Deleting Addresses and Address Groups | 755](#)
- [Services and Service Groups Overview | 758](#)
- [About the Services Page | 758](#)
- [Creating Services and Service Groups | 759](#)
- [Creating Protocols | 761](#)
- [Editing and Deleting Protocols | 765](#)
- [Editing, Cloning, and Deleting Services and Service Groups | 766](#)
- [Application Signatures Overview | 768](#)
- [About the Application Signatures Page | 769](#)
- [Understanding Custom Application Signatures | 770](#)
- [Adding Application Signatures | 772](#)
- [Editing, Cloning, and Deleting Application Signatures | 777](#)
- [Adding Application Signature Groups | 779](#)
- [Editing, Cloning, and Deleting Application Signature Groups | 780](#)
- [About the Departments Page | 781](#)
- [Add a Department | 783](#)
- [Delete a Department | 785](#)
- [About the Protocols Page | 785](#)
- [Add a Protocol Endpoint | 786](#)
- [Edit or Delete Protocol Endpoint | 787](#)

Addresses and Address Groups Overview

An address specifies an IP address or a hostname. You can create addresses that can be used across all policies. Addresses are used in firewall and NAT services and apply to the corresponding policies. If you know only the hostname, you enter it into the **Hostname** field and use the address resolution option to resolve it to an IP address. You can also resolve an IP address to the corresponding hostname.

After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple addresses.

Contrail Service Orchestration (CSO) manages its address book at the global level, assigning objects to devices that are required to create policies. An address book is a collection of addresses and address groups that are available in a security zone. If the device is capable of using a global address book, CSO pushes address objects used in the policies to the global address book of the device.

RELATED DOCUMENTATION

[About the Addresses Page | 751](#)

[Creating Addresses or Address Groups | 753](#)

[Editing, Cloning, and Deleting Addresses and Address Groups | 755](#)

About the Addresses Page

To access this page, select **Configuration > Shared Objects > Addresses**.

Use this page to create, edit, and delete addresses and address groups. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an address or address group. See [“Creating Addresses or Address Groups” on page 753](#).
- Modify, clone, or delete an address or address group. See [“Editing, Cloning, and Deleting Addresses and Address Groups” on page 755](#).

- View the configured parameters of an address or address group. Click the details icon that appears when you hover over the name of an address or address group or select **More > Detailed View**.
- Show or hide columns about the address or address group. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for an address or address group. Click the Search icon in the top right corner of the page to search for an address or address group.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

Table 238 on page 752 provides guidelines on using the fields on the Addresses page.

Table 238: Fields on the Addresses Page

Field	Description
Name	View the name of the address or address group.
Type	View the type of the address or address group.
Hostname	View the hostname of the address.
IP Address	View the IP address associated with the address.
Description	View the description provided about the address or address group when it was created.

RELATED DOCUMENTATION

Addresses and Address Groups Overview 751
Creating Addresses or Address Groups 753
Editing, Cloning, and Deleting Addresses and Address Groups 755

Creating Addresses or Address Groups

Use the **Addresses** page to create addresses and address groups. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

To create an address or address group:

1. Select **Configure > Shared Objects > Addresses**.

The **Addresses** page appears.

2. Click on the add icon (+).

The **Create Addresses** page appears.

3. Complete the configuration according to the guidelines provided in [Table 239 on page 753](#) and [Table 240 on page 755](#).

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new address or address group with your configurations is created. You can use this object in firewall or NAT policies.

Table 239: Fields on the Create Addresses Page

Field	Description
Object Type	Select Address or Address Group. If you select Address Group, then the screen changes so you can select the addresses you want to include in your address group. Table 240 on page 755 describes address group configuration parameters.
Name	Enter a unique name for the address. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your address; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.

Table 239: Fields on the Create Addresses Page (*continued*)

Field	Description
Type	<p>Select a type of address and fill in the corresponding fields. Available types are:</p> <ul style="list-style-type: none"> • Host <ul style="list-style-type: none"> • Host IP—Enter the IPv4 or IPv6 host IP address. For example: 192.0.2.0 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2. If you do not know the IP address, you can enter the hostname and click Look up hostname. • Hostname—Enter the hostname. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed. If you do not know the host name, you can enter the IP address and click Look up IP address. For example, enter www.company.com and click Look up IP address. Hostname lookup is supported for IPv4 and IPv6 addresses. • Range <ul style="list-style-type: none"> • Start Address—Enter a starting IPv4 or IPv6 address for the address range. For example: 192.0.2.0 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2. • End Address—Enter an ending IPv4 or IPv6 address for the address range. The range is validated after you enter the address. <p>NOTE: An address range is configured on a managed device as an address set with one or more network address objects covering the specified address range.</p> • Network <ul style="list-style-type: none"> • Network—Enter the network IP address. For example: 192.0.2.0. IPv6 is also supported. For example: 2001:db8:4136:e378:8000:63bf:3fff:fdd2. • Subnet Mask—Enter the subnet mask for the network range. For example, IPv4 netmask: 192.0.2.0/24. The subnet mask is validated as you enter it. You must enter the correct subnet mask in accordance with the network value. For example, IPv6 netmask: 2001:db8:4136:e378:8000:63bf:3fff:fdd2. • Wildcard <ul style="list-style-type: none"> • Network—Enter the network IPv4 or IPv6 address. For example: 192.0.2.0 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2. • Wildcard Mask—Enter the wildcard mask for the network range. For example: 0.0.0.255. • DNS Host <ul style="list-style-type: none"> • DNS Name—Enter the DNS name. For example: company.com. Only alphanumeric characters, dashes, and periods are accepted. This name cannot exceed 69 characters in length, and must end with an alphanumeric character.

Table 240: Address Group Settings

Field	Description
Object Type	Select Address or Address Group. If you select Address Group, then the screen changes so you can select the addresses you want to include in your address group. Table 239 on page 753 describes address group configuration parameters.
Name	Enter a unique name for the address group. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your address group; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.
Addresses	Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses.

RELATED DOCUMENTATION

[Addresses and Address Groups Overview | 751](#)
[About the Addresses Page | 751](#)
[Editing, Cloning, and Deleting Addresses and Address Groups | 755](#)

Editing, Cloning, and Deleting Addresses and Address Groups

IN THIS SECTION

- [Editing Addresses and Address Groups | 756](#)
- [Cloning Addresses and Address Groups | 756](#)
- [Deleting Addresses and Address Groups | 757](#)

You can edit, clone, and delete addresses and address groups from the **Addresses** page.

Editing Addresses and Address Groups

To modify the parameters configured for an address or address group:

1. Select **Configuration > Shared Objects > Addresses**.

The **Addresses** page appears.

2. Select the address or address group that you want to edit, and then click **More > Edit**, or click the edit icon (pencil symbol) at the right top corner of the table, or right-click and select **Edit**.

The **Edit** page appears, showing the same options as displayed when you create a new address or address group.

3. Modify the parameters according to the guidelines provided in [“Creating Addresses or Address Groups” on page 753](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

When you click **OK**, the modified address or address group is displayed on the **Addresses** page.

NOTE: When you edit an address that is deployed as part of a policy, you will need to redeploy that policy in order for the changes to take effect. See [“Deploying Policies” on page 742](#) for more information.

Cloning Addresses and Address Groups

To clone an address or address group:

1. Select **Configuration > Shared Objects > Addresses**.

The **Addresses** page appears.

2. Right-click the address or address group that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone** page appears with editable fields.

3. Modify the configured parameters of the address or address group, as required.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you select **OK**, the cloned address or address group is saved.

Deleting Addresses and Address Groups

NOTE: Only addresses or address groups that have not been referenced in any policy can be deleted. If you try to delete such an address or address group, an error message will be displayed.

To delete an address or address group:

1. Select **Configuration > Shared Objects > Addresses**.

The **Addresses** page appears.

2. Select the address or address group you want to delete and then click the delete icon **(X)**.

An alert message appears verifying that you want to delete your selection.

3. Click **Yes** to delete the address or address group. If you do not want to delete, click **Cancel** instead.

If you select **Yes**, the selected address or address group is deleted, unless it is referenced in a policy.

RELATED DOCUMENTATION

[Addresses and Address Groups Overview | 751](#)

[About the Addresses Page | 751](#)

[Creating Addresses or Address Groups | 753](#)

Services and Service Groups Overview

A service refers to an application on a device. For example, Domain Name Service (DNS). Services are based on protocols and ports used by an application, and when added to a policy, a configured service can be applied across all devices. Services are candidates for SD-WAN and firewall policy end-points. The protocols used to create a service include: TCP, UDP, MS-RPC, SUN-RPC, ICMP, and ICMPv6. Contrail Service Orchestration (CSO) also includes predefined, commonly used services, and you cannot modify or delete them.

Once you create a service, you can combine it with other services to form a service group. Service groups are useful when you want to apply the same policy to multiple services, as this enables you create fewer policies.

RELATED DOCUMENTATION

[About the Services Page | 758](#)

[Creating Services and Service Groups | 759](#)

[Editing, Cloning, and Deleting Services and Service Groups | 766](#)

About the Services Page

To access this page, select **Configuration > Shared Objects > Services**.

Use the **Services** page to create, modify, clone and delete service or service groups. You can also create and manage protocols, that you use to create services.

A service refers to an application on a device, such as Domain Name Service (DNS). Services are based on protocols and ports used by an application. When added to a policy, a configured service can be applied across all devices. The protocols available to create a service include: TCP, UDP, SUN-RPC, MS-RPC, ICMP, ICMPv6, and so on.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a service or service group. See [“Creating Services and Service Groups” on page 759](#).
- Modify, clone or delete a service or service group. See [“Editing, Cloning, and Deleting Services and Service Groups” on page 766](#).

- View the configured parameters of a service or service group. Click the details icon that appears when you hover over the name of a service or service group, or click **More > Detailed View**.
- Show or hide columns about the services or service groups. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search a specific service or service group. Click the Search icon in the top right corner of the page to search for a service or service group.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

Table 241 on page 759 provides guidelines on using the fields on the **Services** page.

Table 241: Fields on the Service Page

Field	Description
Name	Name of the service or service group.
Type	Specifies whether the object is a service or service group.
Description	Description about the service or service group.
Predefined or Custom	List of predefined services and service groups, and a list of custom services or service groups that you created.

RELATED DOCUMENTATION

- [Services and Service Groups Overview | 758](#)
- [Creating Services and Service Groups | 759](#)
- [Editing, Cloning, and Deleting Services and Service Groups | 766](#)

Creating Services and Service Groups

Use the **Create Service** page to create a service. You can create services based on protocols and ports used by an application. The protocols used to create a service include: TCP, UDP, MS-RPC, SUN-RPC,

ICMP, and ICMPv6. Once you create a service, you can combine it with other services to form a service group. Service groups are useful when you want to apply the same policy to multiple services.

You can also create or modify protocols that you base your services on, from the **Services** page.

To configure a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

2. Click the add icon (+) to create service or service group.

The **Create Services** page appears.

3. Complete the configuration of a service according to the guidelines provided in [Table 242 on page 760](#).

If you want to configure a service group, see [Table 243 on page 761](#).

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new service or service group with the configuration you provided is created. You can use this service or service group as an endpoint in firewall policies.

[Table 242 on page 760](#) provides guidelines on using the fields to create a service.

Table 242: Service Settings

Field	Description
Object Type	Select Service or Service Group . If you select Service Group , then the page changes so you can select the services you want to include in your service group.
Name	Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters; dashes and underscores are allowed.
Description	Enter a description for your service. You should make this description as useful as possible for all administrators.
Protocols	<p>Select the protocol you want to associate with the service. You can use existing protocols that are listed in the Protocols table. You can also create a new protocol, or edit existing protocols:</p> <ul style="list-style-type: none"> • To create a new protocol, click on the add icon (+). See “Creating Protocols” on page 761. • To edit an existing protocol, click on the edit icon (pencil symbol). See “Editing and Deleting Protocols” on page 765.

Table 243 on page 761 provides guidelines on using the fields to create a service group.

Table 243: Service Group Settings

Field	Description
Object Type	Select Service or Service Group . If you select Service Group , then the screen changes so you can select the services you want to include in your service group.
Name	Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters; dashes and underscores are allowed.
Description	Enter a description for your service group. You should make this description as useful as possible for all administrators.
Services	Select the service you want to include in the service group and click the greater-than icon (>) to move the selected service or services from the Available column to the Selected column. You can use the search field at the top of each column to search for listed services.

RELATED DOCUMENTATION

[Services and Service Groups Overview | 758](#)

[About the Services Page | 758](#)

[Editing, Cloning, and Deleting Services and Service Groups | 766](#)

[Creating Protocols | 761](#)

[Editing and Deleting Protocols | 765](#)

Creating Protocols

Use the **Create Protocol** page to create TCP, UDP, MS-RPC, SUN-RPC, ICMP, and ICMPv6 protocols, that can be used in services. A service refers to an application on a device. Services are based on protocols and ports used by an application.

To create a protocol:

1. Select **Configuration > Shared Objects > Services**.
The **Services** page appears.
2. Click the add icon (+) to create service or service group.

The **Create Services** page appears.

3. Click the add icon (+) that appears about the **Protocols** table.

The **Create Protocol** page appears.

4. Complete the configuration of the protocol according to the guidelines provided in [Table 244 on page 762](#) and [Table 245 on page 763](#).
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new protocol with the configuration you provided is created. You can use this protocol to create services.

[Table 244 on page 762](#) provides guidelines on using the fields to create a protocol.

Table 244: Fields on Create Protocol Page Settings

Field	Description
General Information	
Name	Enter a unique name for the protocol. It must begin with an alphanumeric character and cannot exceed 63 characters; dashes and underscores are allowed.
Description	Enter a description for your protocol. It cannot exceed 1,024 characters.
Type	Select the type of the protocol you want to create and fill in the corresponding fields. The available types of protocols are: TCP, UDP, ICMP, SUN-RPC, MS-RPC, ICMPv6, and so on. If you select TCP, continue with this table. See Table 245 on page 763 for the other protocol types.
Destination Port	Enter a destination port number for TCP. The range is from 0 to 65,535.
Advanced Settings	
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds or 2,160 minutes.
ALG	Select an ALG (Application Layer Gateway) service option if applicable.
Source Ports and Port Ranges	Enter the source port or port range for the protocol.

[Table 245 on page 763](#) includes the settings and guidelines for the various protocol types.

Table 245: Create Protocol Type Settings

Field	Description
UDP	
Destination Port	Enter a destination port number for UDP. This is a value or value range from 0 through 65,535.
Advanced Settings	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
ALG	Select an ALG (Application Layer Gateway) service option if applicable.
Source Ports and Port Ranges	Enter a source port or port range for UDP. This is a value or value range from 0 through 65,535.
ICMP	
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
ICMP Type	Enter a value from 0 through 225 for the ICMP message type. For example, enter 1 for host unreachable. You can find these values in RFC 792.
ICMP Code	Enter a value from 0 through 225 for the ICMP code. For example, enter 0 for echo reply. You can find these values in RFC 792.
SUN-RPC	
Destination Port (available if Enable ALG is selected)	Enter a destination port for SUN-RPC. This is a value or value range from 0 through 65,535.
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
Enable ALG	Not selected by default. If you enable ALG for this protocol, you must enter a destination port in the field that becomes available.
RPC Program Number	Enter a value or value range for the RPC (remote procedure call) service. For example, enter 100,017 for remote execution. You can find these values in RFC 5531.
Protocol Type	Select TCP or UDP for the protocol type.

Table 245: Create Protocol Type Settings (*continued*)

Field	Description
MS-RPC	
Destination Port (available if Enable ALG is selected)	Enter a destination port for MS-RPC. This is a value or value range from 0 through 65,535.
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
Enable ALG	Not selected by default. If you enable ALG for this protocol, you must enter a destination port number in the field that becomes available.
UUID	Enter the corresponding UUID value for the MS-RPC service. For predefined values, refer to MS-RPC UUID Mappings.
Protocol Type	Select TCP or UDP for the protocol type.
ICMPv6	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
ICMP Type	Enter a value from 0 through 225 for the ICMPv6 message type. You can find these values in RFC 4443.
ICMP Code	Enter a value from 0 through 225 for the ICMPv6 code. You can find these values in RFC 4443.
Destination Port	Use other to create protocols that do not match the provided type categories. Enter a destination port for the other protocol. This is a value or value range from 0 through 65,535.

RELATED DOCUMENTATION

[Editing and Deleting Protocols | 765](#)
[About the Services Page | 758](#)
[Creating Services and Service Groups | 759](#)

Editing and Deleting Protocols

IN THIS SECTION

- [Editing Protocols | 765](#)
- [Deleting Protocols | 766](#)

You can edit and delete protocols through the **Services** page.

Editing Protocols

To modify the parameters configured for a protocol:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

2. Select the service to which the protocol you want to edit is associated, and click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit Service**.

The **Edit Service** page appears, listing the protocols associated with the service in **Protocols** table.

3. Select the protocol that you want to edit, and then click on the edit icon (pencil symbol) on the right top corner of the **Protocols** table, or right-click and select **Edit Protocol**.

The **Edit Protocol** page appears, showing the same fields as those seen when you create a new protocol.

4. Modify the parameters of the protocol according to the guidelines provided in [“Creating Protocols” on page 761](#).
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the modified protocol appears in the **Protocols** table.

Deleting Protocols

To delete a protocol:

1. Select **Configuration > Shared Objects > Services**.
The **Services** page appears.
2. Select the service to which the protocol you want to delete is associated, and click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit Service**.
The **Edit Service** page appears, listing the protocols associated with the service in **Protocols** table.
3. Select the protocol you want to delete and then click the delete icon (X).
An alert message appears, verifying that you want to delete the protocol.
4. Click **Yes** to delete the protocol. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected protocol is deleted.

RELATED DOCUMENTATION

Services and Service Groups Overview 758
About the Services Page 758
Creating Services and Service Groups 759
Editing, Cloning, and Deleting Services and Service Groups 766
Creating Protocols 761

Editing, Cloning, and Deleting Services and Service Groups

IN THIS SECTION

- [Editing Services and Service Groups | 767](#)
- [Cloning Services or Service Groups | 767](#)
- [Deleting Services and Service Groups | 768](#)

You can edit, clone, and delete services and service groups from the **Services** page.

Editing Services and Service Groups

To modify the parameters configured for a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

2. Select the service or service group that you want to edit, and click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit Service**.

The **Edit Service** page appears, displaying the same options that are displayed when creating a new service or service group.

3. Modify the parameters according to the guidelines provided in [“Creating Services and Service Groups” on page 759](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, you will see the modified service or service group in the **Services** page.

Cloning Services or Service Groups

To clone a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

2. Right-click on the service or service group that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone Service** page appears with editable fields.

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the cloned service or service group will appear beneath the selected service or service group.

Deleting Services and Service Groups

To delete a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

2. Select the service or service group you want to delete and then click the delete icon (X).

An alert message appears, verifying that you want to delete the service or service group.

3. Click **Yes** to delete the service or service group. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected service or service group is deleted.

RELATED DOCUMENTATION

[Services and Service Groups Overview | 758](#)

[About the Services Page | 758](#)

[Creating Services and Service Groups | 759](#)

Application Signatures Overview

Juniper Networks regularly updates the predefined application signature database, making it available to subscribers on the Juniper Networks website. This database includes signature definitions of known application objects that can be used to identify applications for tracking, firewall policies, and quality-of-service prioritization.

Use the **Application Signatures** page to get an overall, high-level view of your application signature settings. You can filter and sort this information to get a better understanding of what you want to configure.

RELATED DOCUMENTATION

[About the Application Signatures Page | 769](#)

[Adding Application Signatures | 772](#)

[Editing, Cloning, and Deleting Application Signatures | 777](#)

[Adding Application Signature Groups | 779](#)

About the Application Signatures Page

To access this page, select **Configuration > Shared Objects > Application Signatures**.

Use the **Application Signatures** page to view application signatures that are already downloaded and to create, modify, clone, and delete custom application signature groups. The **Application Signatures** page displays the name, object type, category and subcategory, risk associated with, and characteristics of the signature. You can create custom application signature groups with a set of similar signatures for consistent reuse when defining policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an application signature. See [“Adding Application Signatures” on page 772](#).
- Modify, clone, or delete an application signature. See [“Editing, Cloning, and Deleting Application Signatures” on page 777](#).
- Add an application signature group. See [“Adding Application Signature Groups” on page 779](#).
- Modify, clone, or delete an application signature group. See [“Editing, Cloning, and Deleting Application Signature Groups” on page 780](#).
- View the configured parameters of an application signature or application signature group. Click the details icon that appears when you hover over the name of an image or click **More > Details**.
- Show or hide columns in the **Application Signatures**. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a specific application signature or application signature group. Click the Search icon in the top right corner of the page to search for an application signature or application signature group.
- Filter the application signature information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Select the filter options; the table displays only the data that fits the filtering criteria.

Field Descriptions

[Table 246 on page 770](#) provides guidelines on using the fields on the **Application Signatures** page.

Table 246: Fields on the Application Signatures Page

Field	Description
Name	Name of the application signature or application signature group.
Object Type	Signature type—either application signature or application signature group.
Category	UTM category of the application signature. For example, the value of Category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Subcategory	UTM subcategory of the application signature. For example, the value of Subcategory can be Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Level of risk associated with the application signature. For example, the value of Risk can be Low, High, unsafe, and so on.
Characteristic	One or more characteristics of the application signature.
Predefined or Custom	A list of predefined application signatures and application signature groups, and a list of custom application signature groups that you created.

RELATED DOCUMENTATION

[Application Signatures Overview | 768](#)

[Adding Application Signatures | 772](#)

[Editing, Cloning, and Deleting Application Signatures | 777](#)

[Adding Application Signature Groups | 779](#)

[Editing, Cloning, and Deleting Application Signature Groups | 780](#)

[Signature Database Overview | 409](#)

[About the Signature Database Page | 410](#)

Understanding Custom Application Signatures

Application identification supports user-defined custom application signatures to detect applications as they pass through the device. Custom application signatures are unique to your environment and are not included in the predefined application package. You use this custom application signature in SD-WAN policies and firewall policies to steer, and block traffic when a threat is detected.

Custom application signatures are required to:

- Control traffic particular to an environment.
- Bring visibility to unknown or unclassified applications.
- Identify Layer 7 applications or temporary applications, and to achieve further granularity of known applications.
- Perform QoS for your specific application.

CSO supports the following custom application signatures:

- **ICMP-Based Mapping**—The Internet Control Message Protocol (ICMP) mapping technique maps standard ICMP message types and optional codes to a unique application name. This mapping technique lets you differentiate between various types of ICMP messages.
- **IP Address-Based Mapping**—Layer 3 and Layer 4 address mapping defines an application by the IP address and optional port range of the traffic.

To ensure adequate security, use address mapping when the configuration of your private network predicts application traffic to or from trusted servers. Address mapping provides efficiency and accuracy in handling traffic from a known application.

With Layer 3 and Layer 4 address-based custom applications, you can match the IP address and port range to destination IP address and port range. When IP address and port range are configured, they must match the destination tuples (IP address and port range) of the packet.

For example, consider a Session Initiation Protocol (SIP) server that initiates sessions from its known port 5060. Because all traffic from this IP address and port is generated by only the SIP application, the SIP application can be mapped to an IP address of the server and port 5060 for application identification. In this way, all traffic with this IP address and port is identified as SIP application traffic.

- **IP Protocol-Based Mapping**—Standard IP protocol numbers can map an application to IP traffic. As with address mapping, to ensure adequate security, use IP protocol mapping only in your private network for trusted servers.
- **Layer 7-Based Signatures**—Layer 7 custom signatures define an application running over TCP or UDP or Layer 7 applications. Layer 7-based custom application signatures are required for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. The custom signature is cacheable for Layer 7 signatures only. You can create multiple signatures and each signature can contain multiple members (maximum 15 members).

Layer 7-based custom application signatures detect applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in SSL, also called Transport Layer Security (TLS). Application identification can extract the server name information or the server certification from the TLS or SSL sessions. It can also detect patterns in TCP or UDP payload in Layer 7 applications.

RELATED DOCUMENTATION

- [Adding Application Signatures | 772](#)
- [Editing, Cloning, and Deleting Application Signatures | 777](#)

Adding Application Signatures

You can add custom application signatures for applications that are not included in Juniper Networks predefined application database. When you add custom application signatures, make sure that your application signatures are unique, by providing a unique and relevant name.

You can add custom application signatures by specifying a name, protocol, port number where the application runs, and match criteria.

To create a custom application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.
2. Click **Create > Signature**.
3. Complete the configuration according to the guidelines provided in [Table 247 on page 772](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new application signature with your configurations is created. You use this application signature while creating SD-WAN policy intents.

[Table 247 on page 772](#) provides guidelines on using the fields on the **Create Application Signature** page.

Table 247: Fields on the Create Application Signature Page

Field	Description
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the application signature.
Signature Order and Priority	

Table 247: Fields on the Create Application Signature Page (*continued*)

Field	Description
Order	<p>Enter the order for the custom application signature. A lower order value has higher priority. This option is used when multiple custom application signatures of the same type match the same traffic. However, you cannot use this option to prioritize among different type of applications such as TCP stream-based applications against TCP port-based applications or IP address-based applications against port-based applications.</p> <p>Range is 1-50000.</p>
Priority	Specify the application signature priority (high or low) over other application signatures.
Signature Classification	
Category	Enter the category of the application signature. For example, Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Sub Category	Enter the subcategory of the application signature. For example, Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Select the level of risk associated with the application signature. For example, low, moderate, high, critical, unsafe, and so on.
Characteristics	Enter one or more characteristics of the application signature. For example, supports file transfer, loss of productivity, and so on.
Application Criteria	<p>Enable one or more application matching criteria:</p> <ul style="list-style-type: none"> • ICMP Mapping • IP Protocol Mapping • Address Mapping • L7 Signature
<i>ICMP Mapping</i>	<p>Click the toggle button to specify the Internet Control Message Protocol (ICMP) value for an application while configuring custom application signatures for application identification.</p> <p>The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. The ICMP code and type provide additional specification, for packet matching in an application definition.</p>
ICMP Type	<p>Enter an ICMP value for the application. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name.</p> <p>Range is 0-254.</p>

Table 247: Fields on the Create Application Signature Page (*continued*)

Field	Description
ICMP Code	<p>Enter an ICMP code for the application. The field provides further information (such as RFCs) about the ICMP type field.</p> <p>Range is 0-254.</p>
<i>IP Protocol Mapping</i>	<p>Click the toggle button to specify the IP protocol value for an application. This parameter is used to identify an application based on its IP protocol value and is intended only for IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.</p>
IP Protocol	<p>Enter an IP Protocol number for the application. Standard IP protocol numbers map an application to IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.</p> <p>Range is 0-254.</p> <p>You can find a complete list of industry standard protocol numbers at the IANA website.</p> <p>NOTE: You cannot use IP protocol numbers 1(ICMP), 6(TCP) and 17(UDP) for custom application signature creation. Instead, we recommend you to use L7 signature policies for these protocols.</p>
<i>Address Mapping</i>	<p>Click the toggle button to specify address mapping information. Layer 3 and Layer 4 address mapping defines an application by matching the destination IP address or port range (optional) of the traffic. Use the address mapping option to configure custom applications signatures when the configuration of your private network predicts application traffic to or from trusted servers.</p> <p>Address mapping provides efficiency and accuracy while handling traffic from a known application. For more information, see Table 248 on page 775.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • You must specify either IP address or TCP/UDP port range for address mapping. • If both IP address and TCP/UDP ports are configured, both should match destination tuples (IP address and port range) of the packet.
<i>L7 Signature</i>	<p>Click the toggle button to specify the Layer 7-based custom application signatures that are required to identify the multiple applications running on the same L7 protocols. Configure a custom signature based on L7 applications. You create Layer 7-based custom application signatures for the identification of multiple applications running on the same L7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. For more information, see Table 249 on page 775.</p>

Table 247: Fields on the Create Application Signature Page (continued)

Field	Description
Cacheable	<p>Click the toggle button to enable caching of application identification results on the device.</p> <p>Enable this option to True only when L7 signatures are configured alone in a custom signature. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.</p>

Table 248: Fields on the Add IP Address Mapping Page

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
IP Address	Enter the destination IPv4 or IPv6 address of the application.
CIDR	<p>Enter a CIDR value for the IP Address that you assign to the application.</p> <p>Range for IPv4 address is 1-32.</p> <p>Range for IPv6 address is 1-128.</p>
TCP Port range	<p>(Optional) Enter space-separated list of ports or port ranges to match a TCP destination port for Layer 3 and Layer 4 address-based custom applications.</p> <p>The range is 0-65535.</p> <p>Example: 80-82 443.</p>
UDP port range	<p>(Optional) Enter space-separated list of ports or port ranges ranges to match an UDP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535.</p> <p>Example: 160-162 260.</p>

Table 249: Fields on the Add Signature Page

Field	Description
Over Protocol	<p>Displays the signature to match the application protocol.</p> <p>Example: HTTP.</p>
Signature Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.

Table 249: Fields on the Add Signature Page (*continued*)

Field	Description
Port Range	<p>Enter the port range for the application.</p> <p>Range is 0-65535</p> <p>Example: 80-82,443</p>
Add Members	Click the plus icon (+) to add the member details.
Member No.	Enter the member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01–m15.)
Context	<p>Select the service-specific context.</p> <ul style="list-style-type: none"> For L7 Signatures over HTTP, select any of the following context: <ul style="list-style-type: none"> http-get-url-parsed-param-parsed http-header-content-type http-header-cookie http-header-host http-header-user-agent http-post-url-parsed-param-parsed http-post-variable-parsed http-url-parsed http-url-parsed-param-parsed For L7 Signatures over SSL, select the service-specific context as ssl-server-name. For L7 Signatures over TCP, select the service-specific context as stream. For L7 Signatures over UDP, select the service-specific context as stream. <p>For possible combinations of context and direction for L7 application creation, refer context (Application Identification).</p>
Direction	<p>Select the direction of the packet flow to which the signature must be matched.</p> <ul style="list-style-type: none"> any—The direction of packet flow can either be from client-side to server-side or from server-side to client-side. client-to-server—The direction of packet flow is from client-side to server-side. server-to-client—The direction of packet flow is from server-side to client-side.
Pattern	Enter the deterministic finite automaton (DFA) pattern matched on the context. The DFA pattern specifies the pattern to be matched for the signature. Maximum length is 128.

RELATED DOCUMENTATION

- [Understanding Custom Application Signatures | 770](#)
- [Editing, Cloning, and Deleting Application Signatures | 777](#)
- [Creating SD-WAN Policy Intents | 575](#)
- [Adding SLA-Based Steering Profiles | 591](#)
- [Adding Path-Based Steering Profiles | 602](#)

Editing, Cloning, and Deleting Application Signatures

IN THIS SECTION

- [Editing Application Signatures | 777](#)
- [Cloning Application Signatures | 778](#)
- [Deleting Application Signatures | 778](#)

You can edit, clone, and delete application signatures from the **Application Signatures** page.

Editing Application Signatures

To modify the parameters configured for a cloned user-created (custom) application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.

The **Application Signatures** page appears.

2. Select the application signature that you want to edit, and then click on the edit icon (pencil), on the top right corner of the table, or right-click and select **Edit Application Signature**.

The **Edit Application Signature** page appears, showing the same options as those displayed when you create a new application signature.

3. Modify the parameters according to the guidelines provided in *Adding Application Signatures*.
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified application signature appears on the **Application Signatures** page.

Cloning Application Signatures

You can clone a custom application signature when you want to reuse an existing application signature, but with a few minor changes. This way, you can save time recreating the application signature from scratch.

To clone a custom application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.

The **Application Signatures** page appears.

2. Select the application signature that you want to clone, and then select **More > Clone**, or right-click the application signature and then select **Clone**.

The **Clone** page appears with editable fields.

3. Modify the fields as required. Refer to the guidelines provided in *Adding Application Signatures*.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The cloned application signature is displayed on the **Application Signatures** page.

Deleting Application Signatures

To delete a cloned user-created (custom) application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.

The **Application Signatures** page appears.

2. Select the application signature you want to delete and then click the delete icon.

An alert message appears to verify that you want to delete the selected application signature.

3. Click **Yes** to delete the selected application signature. If you do not want to delete, click **Cancel** instead.

The deleted application signature is removed from the **Application Signatures** page.

RELATED DOCUMENTATION

[Adding Application Signatures | 772](#)

[Editing, Cloning, and Deleting Application Signatures | 777](#)

Adding Application Signature Groups

Application identification supports custom application signatures to detect applications as they pass through the device. When you add custom signature groups, make sure that your signature groups are unique, by providing a unique and relevant name.

To add an application signature group:

- 1. Select **Configure > Shared Objects > Application Signatures**.
- 2. Click the add icon (+).
- 3. Complete the configuration according to the guidelines provided in [Table 250 on page 779](#).
- 4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new application signature group with your configurations is created. You can use this application signature group in firewall, NAT, and SD-WAN policies.

[Table 250 on page 779](#) provides guidelines on using the fields on the **Create Application Signature Group** page.

Table 250: Fields on the Create Application Signature Group Page

Field	Description
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Group Members	Click the add icon (+) to add signatures to your application group. On the Add Application Signatures page, select the check boxes next to the signatures you want to add to the group.

RELATED DOCUMENTATION

- [Application Signatures Overview | 768](#)
- [About the Application Signatures Page | 769](#)
- [Editing, Cloning, and Deleting Application Signature Groups | 780](#)
- [Signature Database Overview | 409](#)
- [About the Signature Database Page | 410](#)

Editing, Cloning, and Deleting Application Signature Groups

IN THIS SECTION

- [Editing Application Signature Groups | 780](#)
- [Cloning Application Signature Groups | 780](#)
- [Deleting Application Signature Groups | 781](#)

You can edit, clone, and delete application signature groups from the **Application Signatures** page.

Editing Application Signature Groups

To modify the parameters configured for an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

The **Application Signatures** page appears.

2. Select the application signature group that you want to edit, and then select **More > Edit**, or click on the edit icon (pencil symbol), on the top right corner of the table, or right-click and select **Edit**.

The **Edit** page appears, showing the same options as those displayed when you create a new application signature group.

3. Modify the parameters according to the guidelines provided in [“Adding Application Signature Groups” on page 779](#).
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified application signature group appears in the **Application Signatures** page.

Cloning Application Signature Groups

You can clone an application signature group when you want to reuse an existing application signature group, but with a few minor changes. This way, you can save time recreating the application signature group from the start.

To clone an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

The **Application Signatures** page appears.

2. Right-click the application signature group that you want to clone and then select **Clone**, or select **More > Clone**.

The **Clone** page appears with editable fields.

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The cloned application signature group is displayed on the **Application Signatures** page.

Deleting Application Signature Groups

To delete an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

The **Application Signatures** page appears.

2. Select the application signature group you want to delete and then click the delete icon **(X)**.

An alert message appears, verifying that you want to delete the selected item.

3. Click **Yes** to delete the selected application signature group. If you do not want to delete, click **Cancel** instead.

RELATED DOCUMENTATION

[Application Signatures Overview | 768](#)

[About the Application Signatures Page | 769](#)

[Adding Application Signature Groups | 779](#)

[Signature Database Overview | 409](#)

About the Departments Page

To access this page, click **Configuration > Shared Objects > Departments**.

You can use the Departments page to add, view, or delete departments.

A network on a tenant site is divided into multiple LAN segments to improve traffic management and security. A LAN segment is a small portion of a LAN that is used by a work group. You can group LAN

segments as departments for ease of management and for applying specific policies to LAN segments that are members of a department.

You can add one of the following types of departments from the Add Department page:

- A standard department when **Data Center Department** field is selected as **False** (by default).

A standard department can be assigned to a spoke site or an enterprise hub site through directly connected LAN segments only.

- A data center department when you select **Data Center Department** field as **True**.

A data center department is a shared department which enables you to connect to the tenant data center networks and hosts shared resources (for example host servers or web applications) that can be accessed by all the regular departments within the tenant.

A data center department can be assigned to only enterprise hub sites through directly connected or dynamically routed LAN segments (which learn data center routes using OSPF or BGP protocols).

Network segmentation and departments:

If network segmentation is enabled for a tenant (by default), each department within the tenant has its own security zone and Layer 3 VPNs (also called virtual routing and forwarding instances [VRFs]). Since VRFs are isolated for each department in a network segmentation-enabled tenant, Contrail Service Orchestration (CSO) supports overlapping IP addresses across two or more departments. For more information, see [“Overlapping IP Addresses Across Departments” on page 270](#).

NOTE: When a tenant user has overlapping IP addresses configured across departments, access to enterprise hub data center routes requires a source Network Address Translation (NAT) rule with source as an incoming traffic zone (for example, trust) and destination as the data center department zone applied on the enterprise hub device.

If network segmentation is disabled for the tenant, each department has its own security zone but the departments within the tenant share the same Layer 3 VPNs (or VRFs).

Tasks You Can Perform

You can perform the following tasks from this page:

- View detailed information about the department. Click the details icon that appears when you hover over the name of a department or select **More > Detail**.
- Add a Department. See [“Add a Department” on page 783](#).
- Delete a department. See [“Delete a Department” on page 785](#).

- Filter departments. Hover over the filter (funnel) icon, click **Add Filter** to specify the filtering criteria, and click **Add**.

The filtered results are displayed on the same page.

- Search for a department. Click the Search icon in the top right corner of the page.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

- Show or hide columns about a department. Click the **Show/Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.

Field Descriptions

Table 251 on page 783 describes the fields on the **Departments** page.

Table 251: Fields on the Departments Page

Field	Description
Name	Name of the department.
Site/LAN Segments	Sites and LAN segments associated with the department. You can hover over the number link to view the complete list of associated sites and LAN segments.
VPN	Name of the VPN to which the department is assigned.
Data Center	Displays whether the department is a data center department or not (true or false).
Description	Description of the department.
Network UUID	Internal network universally unique identifier (UUID) used by CSO.

RELATED DOCUMENTATION

| [Managing LAN Segments on a Tenant Site](#) | 161

Add a Department

You can add departments from the **Departments** page.

To add a department:

- 1. Click **Configuration > Shared Objects > Departments**.

The Departments page appears.

- 2. Click the **add** icon (+).

The Add Department page appears.

- 3. Complete the configuration settings according to the guidelines provided in [Table 252 on page 784](#).

- 4. Click **OK**.

A confirmation message appears indicating that the department is added successfully.

You are returned to the **Departments** page where the department that you added is displayed.

Table 252: Fields on the Add Department Page

Field	Description
Name	Enter a unique name for the department, which can contain alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.
Description	Enter a description of the department.
VPN	The default VPN to which the department is assigned is displayed. NOTE: This field is displayed only if network segmentation is disabled for the tenant.
Data Center Department	Select whether the department is a data center department (True) or not (False). NOTE: A data center department can be attached (by using LAN segments) only to enterprise hubs.

RELATED DOCUMENTATION

About the Departments Page 781
Delete a Department 785

Delete a Department

You can delete one department at a time from the **Departments** page.

NOTE: You cannot delete a department that is associated with one or more LAN segments or IP VPN configuration in a site. Before you delete the department, you must delete the associated LAN segments and IP VPN configurations. For more information, see [“Managing LAN Segments on a Tenant Site” on page 161](#) and [“Delete IP VPN Configuration from Provider Hubs” on page 186](#).

To delete a department:

1. Click **Configuration > Shared Objects > Departments**.

The Departments page appears.

2. Select the department that you want to delete.

3. Click the delete icon (X).

An alert message appears, asking you to confirm the delete operation.

4. Click **OK**.

A confirmation message appears indicating that the department is deleted successfully and you are returned to the Departments page.

The department is removed from the Departments page.

RELATED DOCUMENTATION

[About the Departments Page](#) | 781

About the Protocols Page

To access this page, click **Configuration > Shared Objects > Protocols**.

You can configure firewall filter terms with protocols (name or value) as source and destination endpoints to permit or block traffic to a specific port.

Use the Protocols page to add, view, or delete protocols.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a protocol. See [“Add a Protocol Endpoint” on page 786](#).
- Edit or delete a protocol. See [“Edit or Delete Protocol Endpoint” on page 787](#).

Field Descriptions

[Table 253 on page 786](#) shows the descriptions of the fields on the **Protocols** page.

Table 253: Fields on the Protocols Page

Field	Description
Protocol	Displays the IPv4 protocol (name or value) for the port.
Description	Displays the description of the protocol.
UUID	Displays the Universally Unique Identifier (UUID) of the protocol.

RELATED DOCUMENTATION

Add a Protocol Endpoint 786
Edit or Delete Protocol Endpoint 787

Add a Protocol Endpoint

Use the Protocols page to add a new protocol, which you can specify as a source endpoint or destination endpoint in firewall filter terms.

To add a protocol:

1. Select **Configuration > Shared Objects > Protocols**.
The Protocols page appears.
2. Click the add icon (+) to add a new protocol.
The Add Protocol Endpoint page appears.

3. Complete the configuration according to the guidelines provided in [Table 254 on page 787](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The new protocol is created. You are returned to the Protocols page where a confirmation message is displayed.

[Table 254 on page 787](#) provides guidelines on using the fields on the **Add Protocol Endpoint** page.

Table 254: Fields on the Add Protocol Endpoint Page

Field	Description
Protocol Number	<p>Enter a valid protocol number.</p> <p>Range is 0-255.</p> <p>Example: egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ospf (89), pim (103), rsvp (46), tcp (6), udp (17)</p>
Description	Enter a description for the protocol.

RELATED DOCUMENTATION

- [About the Protocols Page | 785](#)
- [Edit or Delete Protocol Endpoint | 787](#)

Edit or Delete Protocol Endpoint

IN THIS SECTION

- [Edit Protocols | 788](#)
- [Delete Protocols | 788](#)

You can edit or delete protocols from the **Protocols** page.

Edit Protocols

NOTE: You cannot modify the protocol number.

To modify the parameters configured for a protocol:

1. Select **Configuration > Shared Objects > Protocols**.

The **Protocols** page appears.

2. Select the protocols that you want to edit, and then click on the edit icon (pencil), on the top right corner of the table.

The **Edit Protocol Endpoint** page appears, showing the same options as those displayed when you create a new protocol.

3. Modify the description for the protocol.

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified protocol endpoint description appears on the **Protocols** page.

Delete Protocols

To delete a protocol:

1. Select **Configuration > Shared Objects > Protocols**.

The **Protocols** page appears.

2. Select the protocols that you want to delete and then click the delete icon.

An alert message appears to verify that you want to delete the selected protocols.

3. Click **Yes** to delete the selected protocols. If you do not want to delete, click **No** instead.

The deleted protocol is removed from the Protocols page.

RELATED DOCUMENTATION

[About the Protocols Page | 785](#)

[Add a Protocol Endpoint | 786](#)



Monitoring Jobs and Audit Logs

[Managing Jobs](#) | **791**

[Managing Audit Logs](#) | **797**

Managing Jobs

IN THIS CHAPTER

- [About the Jobs Page | 791](#)
- [Editing and Deleting Scheduled Jobs | 793](#)
- [Viewing Job Details | 795](#)
- [Retrying a Failed Job on Devices | 796](#)

About the Jobs Page

To access this page, click **Monitor > Jobs**.

A job is an action that is performed on any object that is managed by CSO, such as a device, tenant, site, or user. You can monitor the status of jobs that have run or are scheduled to run in CSO. You can run the job immediately or schedule it for a later date and time. You can view the status of the job whether it is completed or failed. You can retry tssm.ztp type jobs that are failed.

Use this page to view the list of all jobs and the jobs that are scheduled to be executed. You can view general information about the jobs and the overall progress and status of the jobs. You can also edit and delete scheduled jobs.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a job. See [“Viewing Job Details” on page 795](#).
- Retry a job. See [“Retrying a Failed Job on Devices” on page 796](#).
- Edit and delete scheduled jobs. See [“Editing and Deleting Scheduled Jobs” on page 793](#).

Field Descriptions

[Table 255 on page 792](#) provides guidelines on using the fields on the Jobs page.

Table 255: Fields on the Jobs Page

Field	Description
Job Name	View the name of the job. CSO automatically generates the job name. Example: MSEC_DOWNLOAD_IPS/APPLICATION_SIGNATURES_08_Jul_17_124229_024
Resource Name	View the resource name of the job. Example: Download IPS/Application Signatures
Status	View the status of the job to know whether the job succeeded, failed, or in progress. Example: Success
Owner	View the name of the owner who created the job. Example: cspadmin
Number of Tasks	View the number of tasks associated with the job. Example: 2 For example, the tasks site.ucpe-32 and customer.sdwan are associated with the job.
Job ID	When a job is initiated from a object in CSO, CSO assigns a unique ID to that job, which serves to identify the job (along with the job type) on the Jobs page. The following is a list of some of the job types supported in CSO: <ul style="list-style-type: none"> • Configure Sites • Download Signature • Create Sites • Remove Site
Start Date	View the start date and time of a task associated with the job.
End State	View the end date and time of a task associated with the job.

Field Descriptions

Table 256 on page 793 provides guidelines on using the fields on the Scheduled Jobs page.

Table 256: Fields on the Scheduled Jobs Page

Field	Description
Schedule ID	View the unique ID of the scheduled job. The value is generated by the database when a new schedule record is inserted into the database. Example: 48
Name	View the unique name of the scheduled job. Example: Tenant Delete_csp.tssm_remove_site_e340354716ae43859fad5ba15669eee2
Status	View the status of the last triggered job. The default status is scheduled.
Record Type	View the job type. Example: tssm onboard tenant
Owner	View the name of the owner who scheduled the job. Example: cspadmin
Next Run Time	View the time when the job is scheduled to run next.

RELATED DOCUMENTATION

[Editing and Deleting Scheduled Jobs | 793](#)

Editing and Deleting Scheduled Jobs

IN THIS SECTION

- [Editing Scheduled Jobs | 794](#)
- [Deleting Scheduled Jobs | 794](#)

You can edit and delete scheduled jobs. This topic contains the following sections:

Editing Scheduled Jobs

You can modify the date and time of deployment of scheduled jobs.

To modify a scheduled job:

1. Select **Monitor > Jobs > Scheduled Jobs**.

The Jobs page displays all scheduled jobs.

2. Select the job that you want to reschedule the deployment, and click the edit icon.

The Edit Schedule page appears. This page displays the option that you have selected initially.

3. Modify the deployment type.

To execute the job immediately, select the **Run now** option.

To reschedule the job for a later date and time, select the **Schedule at a later time** option and select the date and time of deployment.

4. Click **Save** to save the changes.

A success message is displayed indicating that the scheduled job is modified.

Deleting Scheduled Jobs

You can delete one or more scheduled jobs.

To delete a scheduled job:

1. Select **Monitor > Jobs > Scheduled Jobs**.

The Jobs page displays all scheduled jobs.

2. Select the job that you want to delete and then click the delete icon (X). You can select one or more jobs

The Confirm Delete page appears.

3. Click **Yes** to confirm.

A success message is displayed indicating that the scheduled job is deleted.

RELATED DOCUMENTATION

[About the Jobs Page | 791](#)[Viewing Job Details | 795](#)

Viewing Job Details

You can use the Detail for *Job-Name* page to view all the parameters of a job. This page has the following two tabs:

- **Details**—Displays the overall progress of the job and lists general information about the job (for example, the Job ID, Request ID, Created By, and so on). For more information about the field description on this page, see [“About the Jobs Page” on page 791](#).
- **Tasks**—Displays the number of tasks associated with the job. A green check mark (success) or a red cross mark (failed) is displayed next to each task indicating the status of the task. You can click the Detailed View icon to view the summary of the task.

To view details of a job:

- Right-click the job name that you want to see the detailed view for and select **Detail View**.
- Select the job and click **More > Detail View**.
- Alternatively, hover over the job name and click the Detailed View icon that appears before it.

The Detail for *Job-Name* page appears, showing the details of the job and the number of tasks associated with the job. Click **View Logs** to view the status of the jobs. See [“About the Jobs Page” on page 791](#) for a description of each fields on this page.

RELATED DOCUMENTATION

[About the Jobs Page | 791](#)

Retrying a Failed Job on Devices

As a tenant user with the Job Retry capability, you can retry a failed job instead of redoing the tasks involved in the job, to save time.

NOTE: Before you retry a failed job, identify the reason for the failure and then fix it, before retrying the job.

For example, if the bootstrap process failed because the device could not establish an outbound SSH connection, you must fix the problem and ensure that the outbound SSH connection is established before you retry the bootstrap job.

You can retry only the following jobs that did not complete successfully on your devices:

- ZTP jobs
- Bootstrap jobs

To retry a job that was not successful:

1. Select **Monitor > Jobs**.

The Jobs page appears.

2. Select the failed job that you want to retry.

3. Click the **Retry Job** button on the top-right corner of the page.

A retry job is created and executed.

If the job is successful, a confirmation message appears and the job status changes to **Success** on the Jobs page.

RELATED DOCUMENTATION

[About the Jobs Page | 791](#)

[Editing and Deleting Scheduled Jobs | 793](#)

Managing Audit Logs

IN THIS CHAPTER

- [Audit Logs Overview | 797](#)
- [About the Audit Logs Page | 798](#)
- [Viewing the Details of an Audit Log | 799](#)
- [Exporting Audit Logs | 802](#)
- [Purging Audit Logs \(After Archiving or Without Archiving\) | 803](#)

Audit Logs Overview

An audit log is a record of a sequence of activities that have affected a specific operation or procedure. Audit logs are useful for tracing events and for maintaining historical data.

Audit logs contain information about tasks initiated by using the Contrail Service Orchestration (CSO) GUI or APIs. In addition to providing information about the resources that were accessed, audit log entries usually include details about user-initiated tasks, such as the name, role, and IP address of the user who initiated a task, the status of the task, and date and time of execution.

NOTE: Device-driven tasks (that is, tasks not initiated by the user) are not recorded in audit logs.

Administrators can use audit logs to review events. For example, administrators can identify the user accounts associated with an event, determine the chronological sequence of events. For audit log entries that have an associated job, you can click the hyperlinked job ID to go to the Jobs page, where you can view the details of the job.

RELATED DOCUMENTATION

[About the Audit Logs Page | 798](#)

[Exporting Audit Logs | 802](#)

About the Audit Logs Page

To access this page, select **Administration > Audit Logs**.

Use the Audit Logs page to view tasks that you have initiated either by using the Contrail Service Orchestration (CSO) GUI or APIs. You can also export audit logs as a comma-separated values (CSV) file and purge audit logs after archiving them or without archiving them.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of various user-initiated tasks by selecting **More > Details**. You can also mouse over the audit log and click on the **Detailed View** icon. See [“Viewing the Details of an Audit Log” on page 799](#).
- Export audit logs as a CSV file—See [“Exporting Audit Logs” on page 802](#).
- Purge audit logs—See [“Purging Audit Logs \(After Archiving or Without Archiving\)” on page 803](#).
- Search for audit logs by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Sort and filter audit logs:

NOTE: Sorting and filtering is applicable only to some fields.

- Click a column name to sort the audit logs based on the column name.
- Click the filter icon and select whether you want to show or hide column filters or apply a quick filter. For example, you can use audit log filtering to track user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, monitor user login and logout activities over time, and so on.
- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you displayed on the Audit Logs page.

[Table 257 on page 798](#) provides description of the fields on the Audit Logs page.

Table 257: Fields on the Audit Logs Page

Field	Description
Username	Displays the username of the user who initiated the task.

Table 257: Fields on the Audit Logs Page (*continued*)

Field	Description
User IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
Object Name	Displays the name of the object on which the task was initiated. An object can be a tenant, site, device, device image, template, and so on.
Task	Displays the name of the task that triggered the audit log. For example, tenant.create, device.create, site.configure, site.provision, tenant.update, and so on.
Description	Displays details about the task.
Status	<p>Displays the status of the task that triggered the audit log:</p> <ul style="list-style-type: none"> • Success—Job or task was completed successfully. • Failure—Job or task failed and was terminated. • Job Scheduled—Job is scheduled but has not yet started. • Recurring Job Scheduled—Recurring job is scheduled.
End Time	Displays the date and time at which the execution of the task was completed. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.
Job ID	<p>For tasks that have associated jobs, displays the ID of the job associated with the task.</p> <p>You can click the job ID to go to the Jobs page, where you can view the status of the job.</p>

RELATED DOCUMENTATION

[About the Jobs Page](#) | 791

Viewing the Details of an Audit Log

Use the Audit Log Details pane to view details of an audit log.

To view the details of an audit log:

1. Select **Administration > Audit Logs**.

The Audit Logs page appears displaying the audit logs.

- 2. Select the audit log for which you want to view details and click **More > Details**. Alternatively, you can mouse over the audit log, and click on the **Detailed View** icon.

The Audit Log Details pane appears on the right side of the Audit Logs page. [Table 258 on page 800](#) provides descriptions the fields on the Audit Log Details pane.

- 3. Click the close icon (X) to close the Audit Log Details pane.

You are returned to the Audit Logs page.

[Table 258 on page 800](#) provides descriptions the fields on the Audit Log Details pane.

Table 258: Fields on the Audit Log Details Pane

Field	Description
Details	
User	
Username	Displays the user who initiated the task.
User IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
Task	
Task	Displays the name of the task that triggered the audit log. For example, tenant.create, device.create, site.configure, site.provision, tenant.update, and so on.
Status	Displays the status of the task that triggered the audit log: <ul style="list-style-type: none">• Success—Job or task was completed successfully.• Failure—Job or task failed and was terminated.• Job Scheduled—Job is scheduled but has not yet started.• Recurring Job Scheduled—Recurring job is scheduled.
Description	Displays details about the task.
Affected Objects	

Table 258: Fields on the Audit Log Details Pane (*continued*)

Field	Description
Object Name	Displays the name of the affected object on which the task was initiated. An affected object can be a tenant, site, device, device image, template, and so on.. Click the hyperlinked object name to view details of the object: NOTE: If the object is deleted or if you do not have permissions to view it, an error message is displayed.
Object UUID	Displays the Universally Unique Identifier (UUID) of the affected object.
Log Info	
Audit Log ID	Displays the automatically-generated unique ID of the audit log associated with the task.
Job ID	For tasks that have associated jobs, displays the ID of the job associated with the task. You can click the job ID to go to the Jobs page, where you can view the status of the job.
End Time	Displays the date and time at which the task completed execution. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.
Raw Audit Log	
Microservice	Displays the name of the microservice that initiated the task.
Raw Audit Log	Displays all the fields of the audit log that are stored in the database. The raw audit log typically contains additional details or parameters associated with the audit log.

RELATED DOCUMENTATION

[Audit Logs Overview | 797](#)
[About the Audit Logs Page | 798](#)

Exporting Audit Logs

You can export audit logs as a comma-separated values (CSV) file that can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported audit logs, as needed.

To export the audit logs:

1. Select **Administration > Audit Logs**.

The Audit Logs page appears displaying the audit logs.

2. Click **Export**.

The Export Audit Logs page appears.

3. Specify the time period for which you want to export the audit logs according to the guidelines provided in [Table 259 on page 802](#).

NOTE: You can export audit logs for a maximum of 30 days prior to the current date and time. For example, if the current date is May 31, 2018, you can export the audit logs starting from May 1, 2018.

4. Click **OK** to export the audit logs.

Depending on the settings of the browser that you are using, the CSV file containing the audit logs for the specified time period is either downloaded directly, or you are asked to open or save the file.

You are returned to the Audit Logs page.

After the file is downloaded, you can open the CSV file in an application such as Microsoft Excel and view and analyze the logs as required.

Table 259: Fields on the Export Audit Logs Page

Field	Description
Start Date and Time	Specify the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) from when the audit logs should be exported.
End Date and Time	Specify the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) up to when the audit logs should be exported.

RELATED DOCUMENTATION

Audit Logs Overview 797
About the Audit Logs Page 798
Viewing the Details of an Audit Log 799

Purging Audit Logs (After Archiving or Without Archiving)

You can manage the volume of audit log data stored by purging log files from the CSO database without archiving them or by purging log files after archiving them. You can purge audit logs immediately or schedule the purging for a later date and schedule the purging on a recurring basis.

To purge audit logs after archiving or without archiving them:

1. Select **Administration > Audit Logs**.
The Audit Logs page appears displaying the audit logs.
2. Click **Purge**.
The Purge Audit Logs page appears.
3. Complete the configuration according to the guidelines provided in [Table 260 on page 803](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.
You are returned to the Audit Logs page and one of the following operations occur:
 - If you triggered a purge of the audit logs without archiving, a job to purge the audit logs is created.
 - If you triggered a purge of the audit logs after archiving, a job is created to archive the audit logs and then purge the audit logs after archiving.After the audit logs are purged successfully, the Audit Logs page refreshes automatically and displays only the audit logs that were not purged.

Table 260: Purge Audit Logs Settings

Field	Description
Purge Options	

Table 260: Purge Audit Logs Settings (*continued*)

Field	Description
Purge Logs	<p>Select one of the following options to purge audit logs:</p> <ul style="list-style-type: none"> • Purge audit logs that were generated before a specified date and time—If you select this option, you must enter a date and time in the Before field. • Purge generated audit logs that are older than a specified number of days—If you select this option, you must specify the number of days in the Older than field.
Before	<p>To purge audit logs before a specified date and time, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format)</p> <p>You specify the time in the local time zone of the client computer.</p>
Older than	<p>To purge generated audit logs older than a specified number of days, enter the number of days (from 1 through 90)</p>
Archive Logs Before Purging	<p>To archive audit logs <i>before</i> purging them, select this check box. By default, this check box is cleared, which means that audit logs are purged without archiving them.</p> <p>CAUTION: If you choose not to archive the audit logs before purging, the audit logs are deleted from the CSO database and cannot be recovered.</p>
Archive Mode	<p>Specify whether you want to archive the log files locally (local) or on a remote server (remote).</p> <p>If you archive the logs on a remote server, which is the default option, you must enter access and login details for the remote server.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Archived log files are saved in a single file in compressed comma-separated values (CSV) format (extension .zip). • When you archive data locally, the archived log files are saved on the central microservices virtual machine (VM).
Username	Enter a valid username to access the remote server.
Password	Enter a valid password to access the remote server on which the audit logs will be archived.
Confirm Password	For confirmation, re-enter the password to access the remote server.
Remote Server IP Address	Enter the IPv4 address of the remote server; for example, 192.0.2.10.

Table 260: Purge Audit Logs Settings (*continued*)

Field	Description
Remote Server Path	Enter the directory path on the remote server on which to store the archived log files. The directory that you specify must already exist on the remote server.
Schedule Purge	
Type	<p>Specify whether the audit logs should be purged immediately (Run now) or schedule the purge for later (Schedule at a later time).</p> <p>If you schedule the purge for later, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the purge to occur.</p> <p>You specify the time in the local time zone of the client computer.</p>
Recurrence	<p>To specify whether the purge operation should occur on a recurring basis, select this check box.</p> <p>NOTE: This option is enabled only if you choose to archive and purge audit logs older than a specified number of days.</p>
Repeat	Specify the periodicity of the recurrence. Currently, a weekly periodicity is the only option supported.
On	For purges that recur every week, specify one or more days on which you want the purge to recur.
Time	<p>Enter the time (in HH:MM:SS 24-hour or AM/PM format) that you want the recurring purge to occur. By default, the purge recurs at 12.00 AM.</p> <p>You specify the time in the local time zone of the client computer.</p>
Ends	<p>Specify whether the recurring purge ends or not:</p> <ul style="list-style-type: none"> • Select Never to continue (without an end date) the recurring purge operation at the specified recurrence interval. • Select On and enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) on which to stop the recurring purge operation. <p>You specify the time in the local time zone of the client computer.</p>

RELATED DOCUMENTATION

7

PART

Monitoring Alarms, Events, and Threats

[Monitoring Security Alerts and Alarms | 808](#)

[Monitoring Security | 823](#)

[Monitoring SD-WAN Events | 853](#)

[Monitoring Applications | 856](#)

[Monitoring Threats | 875](#)

Monitoring Security Alerts and Alarms

IN THIS CHAPTER

- [About the Monitor Overview Page | 808](#)
- [Alerts Overview | 810](#)
- [About the Generated Alerts Page | 810](#)
- [About the Alert Definitions/Notifications Page | 812](#)
- [Managing Security Alerts Definitions | 813](#)
- [Creating Security Alert Definitions | 814](#)
- [Editing, Cloning, and Deleting Security Alert Definitions | 815](#)
- [About the Alarms Page | 817](#)
- [Enable E-mail Notifications for SD-WAN Alarms | 819](#)
- [Rogue Device Detection | 821](#)

About the Monitor Overview Page

To access this page, click **Monitor > Overview**.

You can use the Monitor Overview page to view information about the alarms and alerts for tenants, network services, connections, and sites on a geographical map. The network operator views the alarms and alerts, and then takes the necessary actions to resolve the issues.

You can also view the visual representation of the hub and link failure on this page.

- **Hub Failure** —The hub and the link connected to the hub appear in red color.
- **Link Failure** — The link connected to the hub appears in red color. However, the hub remains active and appears in green color.

Tasks You Can Perform

You can perform the following tasks from this page:

- View branch site details.
- View on-premise hub site details.
- View cloud spoke sites.
- View provider hub sites.
- View multiple sites.

Field Descriptions

Table 261 on page 809 shows the descriptions of the fields on the Monitor Overview page.

Table 261: Fields on the Monitor Overview Page

Field	Description
Sites	<p>View the sites at which the service is deployed.</p> <p>Click the Sites drop-down list and select Show sites</p>
Connections	<p>View the connections in the network.</p> <p>Click the Connections drop-down list and select Show connections.</p>
Only the node with alerts	<p>View the nodes with issues with the service.</p> <p>Click the drop-down list located next to the Only the nodes with alerts check box and select the type of alerts.</p> <ul style="list-style-type: none">• Critical—Issues that prevent the node from working and require action from the operator. The nodes with critical alerts are displayed in red.• Major—Issues that prevent the node from working at this time, but they do not require action from the operator. The nodes with major alerts are displayed in orange.• Minor—Issues that allow a node to continue working, but not optimally. The network operator may need to take action to resolve the issue. The nodes with minor alerts are displayed in yellow. <p>NOTE: The nodes without any alerts are displayed in blue.</p>

RELATED DOCUMENTATION

Managing Security Alerts Definitions 813
Creating Security Alert Definitions 814

Alerts Overview

Alerts and notifications are used to notify administrators about significant events within the system. Notifications can also be sent through e-mail. You will be notified when a predefined network traffic condition is met. The alert trigger threshold is the number of network traffic events crossing a predefined threshold within a period of time.

Alerts and notifications provide options for:

- Defining alert criteria based on a set of predefined filters. You can use the filters defined in the advanced search to create an alert. You can also save filters and add them to security alert definitions.
- Generating an alert message and notifying you when alert criteria are met.
- Searching for specific alerts on the Generated Alerts page based on alert ID, description, or alert type.
- Supporting event-based alerts.

For example, If you are an administrator, you can define a condition such that if the number of firewall-deny events crosses a predefined threshold in a given time range for a specific device, you will receive an e-mail alert.

NOTE: If a threshold is crossed and remains so for a long duration, new alerts are not generated. Alerts are generated again when the number of logs matching the alert criteria drops below the threshold and crosses the threshold again.

RELATED DOCUMENTATION

[About the Generated Alerts Page | 810](#)

[About the Alert Definitions/Notifications Page | 812](#)

[Managing Security Alerts Definitions | 813](#)

About the Generated Alerts Page

To access this page, click **Monitor > Alerts & Alarms > Alerts**.

Use this page to view the system event-based alerts in response to a configured alert definition. The generated alerts help you to identify problems that appear in your monitored network environment and

displays both security and CSO alerts. You can view statistics such as the number of critical and non-critical alerts.

Tasks You Can Perform

You can perform the following tasks from this page:

- Select the generated alert and then right-click or click **More > Jump to Events and Logs**. The corresponding events that triggered the alert are displayed.
- Select the generated alert and then right-click or click **More > Detail View**. The Alert Detail page appears displaying all the details of the alert.
- Select the generated alert and then right-click or click **More > Clear All Selections**.

Field Descriptions

[Table 262 on page 811](#) provides guidelines on using the fields on the Generated Alerts page.

Table 262: Fields on the Generated Alerts Page

Field	Description
Severity	View the severity of the alert.
Time	View the date and time when the alert was generated.
Site	View the name of the tenant site.
Source	View the source of the alert. The source identifies whether an alert is a security alert or an SD-WAN alert.
Description	View the description of the alert.
Alert Type	View the type of alert.
ID	View the alert ID. Alert ID is a unique identification for each alert. For example, b4a3c027-7157-4861-8e3c-c872721cff2d.
Service Instance	View the service instance associated with the alert..
Object Type	View the object type.
Alert Name	View the name of the alert.
Tenant	View the name of the tenant.

RELATED DOCUMENTATION

| [Managing Security Alerts Definitions | 813](#)

About the Alert Definitions/Notifications Page

To access this page, select **Monitor > Alerts & Alarms > Alert Definitions/Notifications** in the Customer Portal.

Use the Alert Definitions page to manage security alert definitions and enable or disable SD-WAN alarm notifications. An alert definition consists of data criterion for triggering alerts about issues in the SD-WAN environment. Alert definitions also define the necessary action required to resolve issues based on the severity of the alert. An alert is triggered when the event threshold exceeds the data criteria that is defined. You can create an alert definition to monitor your data in real time and identify issues and attacks before they impact your network.

Tasks You Can Perform

You can perform the following tasks from this page:

- Manage Security alert definitions. See [“Managing Security Alerts Definitions” on page 813](#).
- Enable or disable the e-mail notification for alarms. See [“Enable E-mail Notifications for SD-WAN Alarms” on page 819](#).
- Show or hide columns that contain information about security alert definitions. In the Security Alert Definitions tab, click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for alert definitions using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

RELATED DOCUMENTATION

| [Managing Security Alerts Definitions | 813](#)

| [About the Generated Alerts Page | 810](#)

Managing Security Alerts Definitions

Use the Security pane to generate alerts that warn you of problems in your monitored environment. An alert definition consists of data criteria for triggering an alert. An alert is triggered when the event threshold exceeds the data criteria that is defined.

Tasks You Can Perform

You can perform the following tasks from this pane:

- Create security alert definition. See [“Creating Security Alert Definitions” on page 814](#).
- Edit, clone, and delete security alert definition. See [“Editing, Cloning, and Deleting Security Alert Definitions” on page 815](#).

Field Descriptions

[Table 263 on page 813](#) provides guidelines on using the fields on the Security alert definitions pane.

Table 263: Fields on the Security Alert Definitions Pane

Field	Description
Alert Name	View the name of the alert.
Alert Description	View the description for the alert.
Filter	View filter values of the alert.
Recipients	View recipients' e-mail addresses where alert notifications are sent.
Status	View the status of the alert.
Alert Type	View the type of alert. Example: Event-based

RELATED DOCUMENTATION

- [Alerts Overview | 810](#)
- [Creating Security Alert Definitions | 814](#)

Creating Security Alert Definitions

You can create an alert definition to monitor your data in real time. You can identify issues and attacks before they impact your network.

For example, if you are an administrator, you can define a condition such that if the number of firewall deny events crosses a predefined threshold in a given time frame for a specific device, you receive an e-mail alert.

To create a security alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

The Security alert definitions page appears.

2. Click the create icon (+) or add icon (+).

The Create an Alert Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 264 on page 814](#).

4. Click **OK**. If you want to discard the changes, click **Cancel** instead.

A new alert definition with the configured alert triggering condition is created. You can view the generated alerts from the alert definition to troubleshoot the issues with your system.

Table 264: Fields on the Security Alert Definitions Page

Field	Description
General	
Alert Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Alert Description	Enter a description for the alerts; maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system-based.
Status	Select the Active check box to view only the active alerts.
Severity	Select the severity level of the alert: info, minor, major, critical.
Trigger	

Table 264: Fields on the Security Alert Definitions Page (continued)

Field	Description
Use Data Criteria from Filters	<p>Specifies the data criteria from the list of default and user-created filters that are saved from the Event Viewer.</p> <p>To add saved filters:</p> <ul style="list-style-type: none">• Click the Use data criteria from filters link. The Add Saved Filters page appears.• Select the filters to be added.• Click OK.
Add Data Criteria	<p>Specifies the data criteria based on the Time Span period, Group By, and Filter By option. Filtered data only displays the subset of data that meets the criteria that you specify.</p>
Recipient(s)	
E-mail Address(es)	<p>Specify the e-mail addresses for the recipients of the alert notification.</p>
Custom Message	<p>Enter a custom string for identifying the type of alert in the alert notification e-mail.</p>

RELATED DOCUMENTATION

[Managing Security Alerts Definitions | 813](#)

[Editing, Cloning, and Deleting Security Alert Definitions | 815](#)

Editing, Cloning, and Deleting Security Alert Definitions

IN THIS SECTION

- [Editing Security Alert Definitions | 816](#)
- [Cloning Security Alert Definitions | 816](#)
- [Deleting Security Alert Definitions | 816](#)

You can edit, clone, and delete security alert definitions.

Editing Security Alert Definitions

To edit the security alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

The Security Alerts Definition page appears.

2. Select the check box of the security alert definition that you want to modify, and click the edit icon.

The Edit Alert Definition page appears. The options available on the Create Alert Definition page are available for editing.

3. Update the configuration as needed.

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

Cloning Security Alert Definitions

You can clone an alert definition when you want to quickly create a copy of an alert definition and modify its parameters including the name of the alert.

To clone an alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

The Security Alert Definitions page appears.

2. Select the alert definition that you want to clone, and click **More > Clone** at the top right corner of the page.

The Clone Alert Definition page appears. The options available on the Create Alert Definition page are available for editing.

3. Click **OK** to save the configuration.

A new alert definition is created.

Deleting Security Alert Definitions

You can click the delete icon (X) to delete one or more alert definitions.

To delete the alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

The Security Alerts Definition page appears.

2. Select the alert definition that you want to delete and click the delete icon (X icon).

The Confirm Delete page appears.

3. Click **Yes** to delete the alert definition or **No** to cancel the deletion.

If you click **Yes**, then the alert definition is deleted from the main page.

RELATED DOCUMENTATION

[Managing Security Alerts Definitions | 813](#)

[Creating Security Alert Definitions | 814](#)

About the Alarms Page

To access this page, select **Monitor > Alerts & Alarms > Alarms**.

Use the Alarms page to view system-generated alarms. Alarms notify you of conditions that might prevent the device from operating normally. Alarm conditions for a system are preset and are based on the fault monitoring and performance monitoring (FMPM) being performed on a device. For example, conditions such as hardware issues, drop in throughput and latency of data, temperature variations, and capacity optimization issues automatically trigger an alarm.

NOTE: To generate alarms correctly, ensure that CSO and the devices are NTP enabled, and in sync. The time set on CSO must match with the time set on the devices.

The difference between alerts and alarms lies in the type of events that are being monitored. An alert is used to notify administrators about significant events within the system. For example, when a predefined network traffic condition is met. For more information about alerts, see [“Alerts Overview” on page 810](#).

Tasks You Can Perform

You can perform the following tasks from this page:

- View alarm activity within a specific time range:
 - Select either 2 hours (2h), 4 hours (4h), 8 hours (8h), 16 hours (16h), 24 hours (24h), or 1 week (1w), or Custom as the time range to view alarm activity. By default, alarm activity is displayed for a time range of 1 week.

If you click Custom, the Custom Time Range Selection page appears.

You must specify the **From** date and time, and **To** date and time (in MM/DD/YYYY and HH:MM:SS formats).
- View details of an alarm—Select a generated alarm on the page and right-click to select **Detail View** or click **More > Detail View** to view more details (such as alarm type, severity, and so on) of the alarm.
- Delete an alarm—Select an alarm that you want to delete and click the **Delete** icon. The selected alarm is deleted from the page.
- Apply a filter to view specific alarms—Click the **Filter** icon and select the filter criteria from the list of available options, to view only specific alarms. You can filter the alarms based on severity (critical, major, minor, normal), tenant name, site name, and source of the alarm.
- Show or hide columns on the page—Click the **Show or Hide Columns** icon to select or clear columns that you want to display or hide on the page.
- Select the number of alarms that you want to view on the page—From the **Details** list, select either **20**, **50** or **100** as the number of alarms that you want to view on the page.

Field Descriptions

Table 265 on page 818 describes the fields on the Alarms page.

Table 265: Fields on the Alarms Page

Field	Description
Severity	Severity of the alarm.
Time	Date and time when the alarm was generated.
Tenant	Name of the tenant.
Site	Name of the tenant site for which the alarm was generated.
Source	Source from where the alarm originated.

Table 265: Fields on the Alarms Page (*continued*)

Field	Description
Description	Description of the alarm.
UUID	Universally Unique Identifier (UUID) of the alarm. You can use the UUID to identify an alarm on the Monitor > Logs page.
Link Name	Name of the link that generated the alarm.
Service Instance	Service instance associated with the alarm.
Object Type	Type of device from which the alarm originated. Example: Hub

Enable E-mail Notifications for SD-WAN Alarms

Starting from CSO Release 5.1.1, you now notify the user (tenant administrators and tenant operators) about SD-WAN alarms. You can also specify the minimum severity level of alarms that must be notified to the users. Alarm notifications enable users to take action to ensure that the network runs smoothly.

NOTE: You can enable or disable the e-mail notification for SD-WAN alarms if you are an SP administrator, or OpCo administrator, or tenant administrator.

To enable e-mails notifications for SD-WAN alarms:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications**.

The Definitions/Notifications page appears.

2. Select the **SD-WAN Alarm Notifications** tab.

The SD-WAN Alarm Notifications page appears.

3. Complete the configuration according to the guidelines provided in [Table 266 on page 820](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **Save** to save the changes.

If you have enabled e-mail notifications, an e-mail will be sent to the user based on the severity level that you specified for an alarm.

If you have disabled e-mail notifications, the users will not receive e-mail notifications in case of alarms.

Table 266: SD-WAN Alarm Notifications Settings

Field	Description
Send Email Notifications	<p>Click the toggle button to enable or disable the e-mail notifications of alarms to users. By default, e-mail notifications are disabled.</p> <p>After enabling this field, you must specify the minimum severity level of the alarm and select the e-mail addresses of the users.</p>
Minimum Severity to Report	<p>Select the minimum severity level (critical, major, minor) of the alarms to users through an e-mail.</p> <ul style="list-style-type: none"> • Critical—If you select this option, e-mail notifications are sent to users only for alarms with the severity level critical. • Major—If you select this option, e-mail notifications are sent to users only for alarms with the severity levels major or critical. • Minor—If you select this option, e-mail notifications are sent to users only for alarms with the severity levels minor, major, or critical.
Recipients	<p>Select one or more e-mail addresses of the users from the list. Only users with tenant administrator or tenant operator roles are listed.</p> <p>The e-mail addresses listed are based on the users that are listed in the Administration > Users page.</p>

Release History Table

Release	Description
5.1.1	Starting from CSO Release 5.1.1, you now notify the user (tenant administrators and tenant operators) about SD-WAN alarms. You can also specify the minimum severity level of alarms that must be notified to the users. Alarm notifications enable users to take action to ensure that the network runs smoothly.

RELATED DOCUMENTATION

[About the Alert Definitions/Notifications Page](#) | 812

Rogue Device Detection

Starting in Release 6.1.0, CSO detects any unauthorized device that attempts to access the network. On detection, CSO immediately rejects the connection request from the device and generates an alarm so that administrators can take remedial actions promptly.

CSO generates an alarm indicating unauthorized access in the following scenarios:

- **Scenario 1:** An unauthorized device attempts to connect using the configuration of a device that is modeled but not yet provisioned on CSO.

Users might create (model) a site and provision (activate) the site later. In such a case, the device (for example, device A) at the site is not connected to the CSO network. If a rogue device attempts to connect to the CSO network by using the configuration of device A, CSO rejects the connection request and generates an alarm.

Users can clear the alarm in the **Monitor > Alerts & Alarms** page after taking the necessary actions such as blocking the traffic originating from the rogue device.

CSO clears the alarm automatically when the original device is provisioned and connected to CSO.

The alarm message that is displayed for this scenario is as follows:

```
Rejected connection from an unauthorized device! A device with serial number
serial number of rogue device attempted to connect to CSO as device A registered
with CSO with serial number serial number of device A. Verify the serial number
in the stage 1 configuration applied on the device or if the device is an
unauthorized one, take immediate action to block the device.
```

- **Scenario 2:** An unauthorized device attempts to connect using the configuration of a device that is provisioned on the CSO network.

If a device attempts to connect to the CSO network using the configuration of a provisioned device, CSO identifies the device as a rogue device and rejects the connection. CSO also raises an alarm to notify the users. Users can clear the alarm in the **Monitor > Alerts & Alarms** page after taking the necessary actions to block the device from accessing the network again.

The alarm message that is displayed for this scenario is as follows:

Rejected connection request from an unauthorized device! A device with serial number *serial number of rogue device* and device ID *device id of rogue device* attempted to connect to CSO. A device with the same device ID and serial number *serial number of provisioned device* is already provisioned on CSO. Take immediate action to prevent the unauthorized device from accessing your network again.

Monitoring Security

IN THIS CHAPTER

- [About the All Security Events Page | 823](#)
- [About the Firewall Events Page | 828](#)
- [About the Web Filtering Events Page | 831](#)
- [About the IPsec VPNs Events Page | 834](#)
- [About the Content Filtering Events Page | 836](#)
- [About the Antispam Events Page | 838](#)
- [About the Antivirus Events Page | 840](#)
- [About the IPS Events Page | 843](#)
- [About the Screen Events Page | 846](#)
- [About the Traffic Logs Page | 850](#)

About the All Security Events Page

To access this page, click **Monitoring > Security Events > All Events**.

Use this page to get an overall, high-level view of your network environment. You can view abnormal events, attacks, viruses, or worms when log data is correlated and analyzed.

This page provides administrators with an advanced filtering mechanism and provides visibility into actual events collected by the Log Collector. Using the time-range slider, you can instantly focus on areas of unusual activity by dragging the time slider to the area of interest to you. The slider and the Custom button under Time Range remain at the top of each tab. Users select the time range, and then they can decide how to view the data, using the summary view or detail view tabs.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all events in your network. See [“Summary View” on page 824](#).

- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 824](#).

Summary View

You can view a brief summary of all the events in your network. At the center of the page is critical information, including total number of events, viruses found, total number of interfaces that are down, number of attacks, CPU spikes, and system reboots. This data is refreshed automatically based on the selected time range. At the bottom of the page is a swim lane view of different events that are happening at a specific time. The events include firewall, web filtering, VPN, content filtering, antispam, antivirus, and IPS. Each event is color-coded, with darker shades representing a higher level of activity. Each tab provides deep information like type, and number of events occurring at that specific time.

[Table 267 on page 824](#) describes the widgets on the All Events Summary View page.

Table 267: Widgets on the All Events Summary View Page

Field	Description
Total Events	View the total number of all the events that includes firewall, web filtering, IPS, IPSec VPNs, content filtering, antispam, and antivirus events.
Virus Instances	View the total number of virtual instances running in the system.
Attacks	View the total number of attacks on the firewall.
Interface Down	View the total number of interfaces that are down.
CPU Spikes	View the total number of times a CPU utilization spike has occurred.
Reboots	View the total number of system reboots.
Sessions	View the total number of sessions established through firewall.

Detail View

Click **Detail View** for comprehensive details of events in a tabular format that includes sortable columns. You can sort the events using the Group By option. For example, you can sort the events based on severity. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

Advanced Search

You can perform advanced search of all events using the text field present above the tabular column. It includes the logical operators as part of the filter string. Enter the search string in the text field and based on your input, a list of items from the filter context menu is displayed. . You can select a value from the list and then select a valid logical operator to perform the advanced search operation Press Enter to display the search result in the tabular column below.

To delete the search string in the text field, click the delete icon (X icon).

Examples of event log filters are shown in the following list:

- Specific events originating from or landing within United States

Source Country = United States OR Destination Country = United States AND Event Name = IDP_ATTACK_LOG_EVENT, IDP_ATTACK_LOG_EVENT_LS, IDP_APPDDOS_APP_ATTACK_EVENT_LS, IDP_APPDDOS_APP_STATE_EVENT, IDP_APPDDOS_APP_STATE_EVENT_LS, AV_VIRUS_DETECTED_MT, AV_VIRUS_DETECTED, ANTISPAM_SPAM_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT_LS, FWAUTH_FTP_USER_AUTH_FAIL, FWAUTH_FTP_USER_AUTH_FAIL_LS, FWAUTH_HTTP_USER_AUTH_FAIL, FWAUTH_HTTP_USER_AUTH_FAIL_LS, FWAUTH_TELNET_USER_AUTH_FAIL, FWAUTH_TELNET_USER_AUTH_FAIL_LS, FWAUTH_WEBAUTH_FAIL, FWAUTH_WEBAUTH_FAIL_LS

- User wants to filter all RT flow sessions originating from IP addresses in specific countries and landing on IPs in specific countries

Event Name = RT_FLOW_SESSION_CREATE, RT_FLOW_SESSION_CLOSE AND Source IP = 177.1.1.1, 220.194.0.150, 14.1.1.2, 196.194.56.4 AND Destination IP = 255.255.255.255, 10.207.99.75, 10.207.99.72, 223.165.27.13 AND Source Country = Brazil, United States, China, Russia, Algeria AND Destination Country = Germany, India, United States

- Traffic between zone pairs for policy – IDP2

Source Zone = trust AND Destination Zone = untrust, internal AND Policy Name = IDP2

- UTM logs coming from specific source country, destination country, source IP addresses with or without specific destination IP addresses.

Event Category = antispam, antivirus, contentfilter, webfilter AND Source Country = Australia AND Destination Country = Turkey, United States, Australia AND Source IP = 1.0.0.0, 1.1.1.3 OR Destination IP = 74.125.224.47, 5.56.17.61

- Events with specific sources IPs or events hitting HTP, FTP, HTTP, and unknown applications coming from host DC-SRX1400-1 or VSRX-75.

Application = tftp, ftp, http, unknown OR Source IP = 192.168.34.10, 192.168.1.26 AND Hostname = dc-srx1400-1, vsrx-75

[Table 268 on page 826](#) describes the fields on the All Events Detail View Page.

Table 268: Fields on the All Events Detail View Page

Field	Description
Time	View the time when the log was received.
Event Name	View the event name of the log.
Site	View the name of the tenant site.
Source Country	View the source country name.
Source IP	View the source IP address from where the event occurred.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack Name	View the attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	View the severity level of the threat.
Policy Name	View the policy name in the log.
UTM Category or Virus Name	View the UTM category of the log.
URL	View the accessed URL name that triggered the event.
Event Category	View the event category of the log.
User Name	View the username of the log.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source.
Application	View the application name from which the events or logs are generated
Hostname	View the hostname in the log.

Table 268: Fields on the All Events Detail View Page (*continued*)

Field	Description
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the nested application in the log.
Source Zone	View the source zone of the log.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
Roles	View the role name associated with the log.
Reason	View the reason for the log generation. For example, a connection tear down may have an associated reason such as “authentication failed”.
NAT Source Port	View the translated source port.
NAT Destination Port	View the translated destination port.
NAT Source Rule Name	View the NAT source rule name.
NAT Destination Rule Name	View the NAT destination rule name.
NAT Source IP	View the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	View the translated (also called natted) destination IP address.
Traffic Session ID	View the traffic session ID of the log.
Path Name	View the path name of the log.
Logical system Name	View the name of the logical system.
Rule Name	View the name of the rule.
Profile Name	View the name of the All events profile that triggered the event.

RELATED DOCUMENTATION

[About the Firewall Events Page | 828](#)

[About the Web Filtering Events Page | 831](#)

[About the IPsec VPNs Events Page | 834](#)

[About the Content Filtering Events Page | 836](#)

[About the Antispam Events Page | 838](#)

[About the Antivirus Events Page | 840](#)

[About the IPS Events Page | 843](#)

About the Firewall Events Page

To access this page, click **Monitor > Security Events > Firewall**.

Use the Firewall Events page to view information about security events based on firewall policies. Analyzing firewall logs yields useful security management information, such as attempts to breach your network and observing the inherent characteristics of your traffic in real-time. Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the firewall events in your network. See [“Summary View” on page 828](#)
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 829](#).

Summary View

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all firewall events and dark blue lanes represent blocked firewall events.

Below the swim lanes are widgets displaying critical information such as top sources, top destinations, top users, and top reporting devices.

[Table 269 on page 829](#) describes the widgets on the Summary View page.

Table 269: Widgets on the Summary View Page

Widget	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.
Top Users	View then top users of the network traffic; sorted by event count.
Top Reporting Devices	View the top reporting devices in the network; sorted by event count.

Detail View

Detail view includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected

[Table 270 on page 829](#) provides guidelines on using the fields on the Detail View page.

Table 270: Fields on the Detail View Page

Field	Description
Time	View the time when the log was received.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Policy Name	View the policy name in the log.

Table 270: Fields on the Detail View Page (*continued*)

Field	Description
User Name	View the username of the log.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Application	View the application name from which the events or logs are generated.
Hostname	View the hostname in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the nested application in the log.
Source Zone	View the user traffic received from the zone.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
Roles	View the role names associated with the event.
NAT Source Port	View the translated source port.
NAT Destination Port	View the translated destination port.
NAT Source Rule Name	View the NAT source rule name.
NAT Destination Rule Name	View the NAT destination rule name.
NAT Source IP	View the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	View the translated (also called natted) destination IP address.
Traffic Session ID	View the traffic session ID of the log.
Rule Name	View the rule name of the log.

RELATED DOCUMENTATION

About the All Security Events Page 823
About the Web Filtering Events Page 831
About the IPsec VPNs Events Page 834
About the Content Filtering Events Page 836
About the Antispam Events Page 838
About the Antivirus Events Page 840
About the IPS Events Page 843

About the Web Filtering Events Page

To access this page, click **Monitor > Security Events > Web Filtering**.

Use the Web Filtering page to view information about security events based on Web filtering policies. Web filtering allows you to permit or block access to specific websites by URL or by URL category using cloud-based lookups, a local database, or an external Websense server. Analyzing Web filtering logs yields useful security management information such as users detected accessing restricted URLs and actions taken by the system. Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the Web filtering events in your network. See [“Summary View” on page 831](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 832](#).

Summary View

The top of the page has a swim lane graph of all the Web filtering events against the blocked events.

Below the swim lanes are widgets displaying critical information such as top sources, top destinations, top users, and top reporting devices.

You can use the widgets at the bottom of the page to view critical information such as top URLs blocked, top matched profiles, top sources, and top destinations.

[Table 271 on page 832](#) describes the widgets on the Summary View page.

Table 271: Widgets on the Summary View Page

Widget	Description
Top URLs blocked	View the URL names that are blocked; sorted by event count.
Top Matched Profiles	View the web filtering profile names; sorted by event count.
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.

Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 272 on page 832](#) provides guidelines on using the fields on the Detail View page.

Table 272: Fields on the Detail View Page

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.

Table 272: Fields on the Detail View Page (*continued*)

Fields	Description
Description	View the description of the log.
UTM category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
Path Name	View the path name of the log.
Profile Name	View the name of the Web filtering profile that triggered the event.

RELATED DOCUMENTATION

[About the All Security Events Page | 823](#)
[About the Firewall Events Page | 828](#)
[About the IPsec VPNs Events Page | 834](#)
[About the Content Filtering Events Page | 836](#)
[About the Antispam Events Page | 838](#)
[About the Antivirus Events Page | 840](#)
[About the IPS Events Page | 843](#)

About the IPsec VPNs Events Page

To access this page, click **Monitor > Security Events > IPsec VPNs**.

Use this page to view information about security events based on IPsec VPN policies. The event viewer provides a view of all IPsec VPN events.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the IPsec VPN events in your network. See [“Summary View” on page 834](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 835](#).

Summary View

The top of the page has a swim lane graph of all the VPN events. You can use the widgets at the bottom of the page to view critical information such as top sources, top destinations, and top reporting devices.

[Table 273 on page 834](#) describes the widgets on the Summary View page.

Table 273: Widgets on the Summary View Page

Widget	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.
Top Reporting Devices	View the top reporting device IP addresses; sorted by event count.

Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, log source, host name, source country, and so on.

[Table 274 on page 835](#) provides guidelines on using the fields on the Detail View page.

Table 274: Fields on the Detail View Page

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Destination Country	View the destination country name from where the event occurred.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Rule Name	View the name of the antivirus profile that triggered the event.

RELATED DOCUMENTATION

[About the All Security Events Page | 823](#)

[About the Firewall Events Page | 828](#)

[About the Web Filtering Events Page | 831](#)

[About the Content Filtering Events Page | 836](#)

[About the Antispam Events Page | 838](#)

[About the Antivirus Events Page | 840](#)

[About the IPS Events Page | 843](#)

About the Content Filtering Events Page

To access this page, click **Monitor > Security Events > Content Filtering**.

Use this page to view information about security events based on content filtering policies. The event viewer provides a view of all content filtering events and how the events are handled by content filter. This page can be used to view traffic on the network in real time or as a debugging tool to view how content filtering is operating.

Content filtering provides basic data loss prevention functionality. Content filtering screens traffic based on MIME type, file extension, protocol commands, and embedded object type. It either permits or blocks specific commands or extensions on a protocol-by-protocol basis.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the content filtering events in your network. See [“Summary View” on page 836](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 837](#).

Summary View

The top of the page has a swim lane graph of all the content filtering events against the blocked events. You can use the widgets at the bottom of the page to view critical information such as top blocked protocol commands, top reasons, and top sources.

[Table 275 on page 836](#) describes the widgets on the Summary View page.

Table 275: Widgets on the Summary View Page

Widget	Description
Top Blocked Protocol commands	View the top command names or file extensions blocked on a protocol-by-protocol basis.
Top Reasons	View the top reasons for blocking the content. For example: Inappropriate or harmful communication.

Table 275: Widgets on the Summary View Page (*continued*)

Widget	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.

Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 276 on page 837](#) provides guidelines on using the fields on the Detail View page.

Table 276: Fields on the Detail View Page

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Description	View the description of the log.
UTM Category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access

Table 276: Fields on the Detail View Page (*continued*)

Fields	Description
Profile Name	View the name of the content filtering profile that triggered the event.

RELATED DOCUMENTATION

- [About the All Security Events Page | 823](#)
- [About the Firewall Events Page | 828](#)
- [About the Web Filtering Events Page | 831](#)
- [About the IPsec VPNs Events Page | 834](#)
- [About the Antispam Events Page | 838](#)
- [About the Antivirus Events Page | 840](#)
- [About the IPS Events Page | 843](#)

About the Antispam Events Page

To access this page, click **Monitor > Security Events > Antispam**.

Use this page to view information about security events based on antispam policies. The event viewer provides a view of all antispam events and the action taken by the antispam scanner.

The antispam scanner inspects and block spam by scanning inbound and outbound SMTP e-mail traffic. The filtering can be server-based using an external spam block list server or local-based using local lists (blocklists and allowlists) for matching.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the antispam events in your network. See [“Summary View” on page 839](#).

- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 839](#).

Summary View

The top of the page has a swim lane graph of all antispam events. You can use the widget at the bottom of the page to view source IP addresses of the network traffic, sorted by event count.

Detail View

You can aggregate the events using the Group by option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 277 on page 839](#) provides guidelines on using the fields on the Detail View page.

Table 277: Fields on the Detail View Page

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Description	View the description of the log.
UTM Category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.

Table 277: Fields on the Detail View Page (*continued*)

Fields	Description
Reason	View the reason for the log generation. For example, unrestricted access
Profile Name	View the name of the content filtering profile that triggered the event.

RELATED DOCUMENTATION

[About the All Security Events Page | 823](#)

[About the Firewall Events Page | 828](#)

[About the Web Filtering Events Page | 831](#)

[About the IPsec VPNs Events Page | 834](#)

[About the Content Filtering Events Page | 836](#)

[About the Antivirus Events Page | 840](#)

[About the IPS Events Page | 843](#)

About the Antivirus Events Page

To access this page, click **Monitor > Security Events > Antivirus**.

Use this page to view information about security events based on antivirus policies. The event viewer provides a view of all antivirus events and the action taken by the virus scanner.

The antivirus scanner inspects files transmitted over several protocols to determine if the files exchanged are malicious (for example, viruses, Trojans, rootkits, and worms).

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the antivirus events in your network. See [“Summary View” on page 841](#).

- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 841](#).

Summary View

The top of the page has a swim lane graph of all the antivirus events against the blocked events. You can use the widgets at the bottom of the page to view critical information such as top blocked protocol commands, top reasons, and top sources.

[Table 278 on page 841](#) provides guidelines on using the widgets on the Detail View page.

Table 278: Widgets on the Summary Page

Field	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.
Top Reporting/Attacked Devices	View the top reporting/attacked device IP addresses; sorted by event count.
Top Viruses	View the top virus names detected; sorted by event count.
Top Source Countries	View the top source country names where the events originated; sorted by event count.
Top Destination Countries	View the top destination country names where the events occurred; sorted by event count.

Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 279 on page 841](#) provides guidelines on using the fields on the Detail View page.

Table 279: Fields on the Detail View Page

Fields	Description
Time	View the time when the event occurred.

Table 279: Fields on the Detail View Page (*continued*)

Fields	Description
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
UTM Category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
Profile Name	View the name of the antivirus profile that triggered the event.

RELATED DOCUMENTATION

[About the All Security Events Page | 823](#)
[About the Firewall Events Page | 828](#)

About the Web Filtering Events Page	831
About the IPsec VPNs Events Page	834
About the Content Filtering Events Page	836
About the Antispam Events Page	838
About the IPS Events Page	843

About the IPS Events Page

To access this page, click **Monitor > Security Events > IPS**.

Use the IPS Events page to view information about security events based on IPS policies. Analyzing IPS logs yields useful security management information, such as abnormal events, attacks, viruses, or worms.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the all the IPS events in your network. See [“Summary View” on page 843](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 844](#).

Summary View

The data presented in the area graph is refreshed automatically based on the selected time range. You can use widgets to view critical information such as IPS severities, top sources, top destinations, top reporting devices, top IPS attacks, top source countries, and top destination countries.

[Table 280 on page 843](#) provides guidelines on using the widgets on the Detail View page.

Table 280: Widgets on the Summary Page

Field	Description
IPS Severities	View the top IPS severities of the events based on the severity level: high, medium, low.

Table 280: Widgets on the Summary Page (continued)

Field	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by the number of event occurrences.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by the number of event occurrences.
Top Reporting/Attacked Devices	View the top devices that are attacked by IPS events; sorted by the number of times users are active on the network.
Top IPS attacks	View the top IPS attacks in the network traffic; sorted by the times devices are attacked.
Top Source Countries	View the top source countries from where the event source originated; sorted by the number of IP addresses.
Top Destination Countries	View the top source countries from where the event source originated; sorted by the number of IP addresses.

Detail View

You can sort the events using the Group By option. For example, you can sort the events based on severity. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

[Table 281 on page 844](#) provides guidelines on using the fields on the Detail View page.

Table 281: Fields on the Detail View Page

Column	Description
Time	View the time when the log was received.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event.

Table 281: Fields on the Detail View Page (*continued*)

Column	Description
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack name	View the attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	View the threat severity of the event.
Policy Name	View the policy name in the log.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source.
Application	View the application name from which the events or logs are generated.
Hostname	View the host name in the log.
Service Name	View the name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the nested application name in the log.
Source Zone	View the source zone of the log.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
NAT Source Port	View the translated source port.
NAT Destination Port	View the translated destination port
NAT Source IP	View the NAT source IP address of the log.
NAT Destination IP	View the NAT destination IP address of the log.
Rule Name	View the name of the rule.

RELATED DOCUMENTATION

[About the All Security Events Page | 823](#)

[About the Firewall Events Page | 828](#)

[About the Web Filtering Events Page | 831](#)

[About the IPsec VPNs Events Page | 834](#)

[About the Content Filtering Events Page | 836](#)

[About the Antispam Events Page | 838](#)

[About the Antivirus Events Page | 840](#)

About the Screen Events Page

To access this page, click **Monitor > Security Events > Screen**.

Use this page to view information about screen events that occur as a result of the screen options configured on SRX Series or vSRX security devices. Screen options are a detection and defense mechanism configured to filter the connection attempts bound towards a security zone. Screen options are used to prevent attacks, such as IP address sweeps, port scans, denial of service (DOS) attacks, Internet Control Message Protocol (ICMP), UDP, and SYN (Synchronize) floods.

You can view information related to screen events, including ICMP screening, IP screening, TCP screening, and UDP screening.

Using the time-range slider, you can quickly focus on the time and area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the **Custom** button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the screen events in your network. See [“Summary View” on page 847](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 847](#).

Summary View

The top of the page has a swim lane graph of all the screen events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries.

[Table 282 on page 847](#) describes the widgets on the Detail View page.

Table 282: Widgets on the Summary Page

Field	Description
Top Sources	Top five source IP addresses with highest network traffic.
Top Destinations	Top five destination IP addresses with highest network traffic.
Top Source Countries	Top five countries from which the traffic that triggered the highest number of events originated and the number of events per country.
Top Destination Countries	Top five countries to which the traffic that triggered the highest number events was sent and the number of events per country.

Detail View

You can group the events using the **Group By** option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 283 on page 847](#) describes the fields on the Detail View page.

Table 283: Fields on the Detail View Page

Fields	Description
Log Generated Time	Time when the event occurred.
Log Received Time	Time the log was received at the log collector.
Site	Name of the tenant site from which the event originated.
Event Name	Name of the device event in the log.
Source Country	Country from which the traffic that triggered the event originated.
Source IP	Source IP address for the traffic that triggered the event (IPv4 or IPv6).

Table 283: Fields on the Detail View Page (*continued*)

Fields	Description
Destination Country	Country to which the traffic that triggered the event was sent.
Destination IP	Destination IP address for the traffic that triggered the event (IPv4 or IPv6).
Source Port	Source TCP/UDP port number of the traffic that triggered the event.
Destination Port	Destination TCP/UDP port number of the traffic that triggered the event.
Attack Name	Name of the attack in the log for threat event. For example, trojan, worm, virus, and so on.
Description	Brief description of the event.
Threat Severity	Level of severity of the threat. For example, minor, major, critical, and so on.
Policy Name	Name of the policy which generates the log. The policy is configured on the SRX Series or vSRX device.
Virus Name	This field is not applicable for screen events.
URL	Accessed URL that triggered the event.
Event Category	Event category in the log. For example, screen.
User Name	User name identified by the SRX Series or vSRX device, if user identity is enabled on the device.
Argument	Type of traffic. For example, FTP and HTTP.
Action	Action taken for the event. For example, warning, allow, and block.
Log Source	IP address of the device where the log is received (IPv4 or IPv6).
Application	Name of the application associated with the traffic that triggered the event.
Host Name	Hostname of the device where the log was generated.
Service Name	Name of the application service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Nested Application	Nested application associated with the traffic that triggered the event.

Table 283: Fields on the Detail View Page (*continued*)

Fields	Description
Source Zone	Source security zone of the traffic that triggered the event.
Destination Zone	Destination security zone of the traffic that triggered the event.
Protocol ID	Protocol ID of the traffic that triggered the event.
Roles	Roles of the user as defined in the Active Directory, if available.
Reason	Reason for the log generation. For example, unrestricted access.
NAT Source Port	Translated source port.
NAT Destination Port	Translated destination port.
NAT Source Rule Name	NAT source rule name configured on the SRX Series or vSRX device.
NAT Destination Rule Name	NAT destination rule name configured on the SRX Series or vSRX device.
NAT Source IP	Translated source IP address for the traffic that triggered the event (IPv4 or IPv6).
NAT Destination IP	Translated destination IP address for the traffic that triggered the event (IPv4 or IPv6).
Traffic Session ID	Traffic session ID of the log.
Path Name	This field is not applicable for screen events.
Logical System Name	Name of the logical system which received the log.
Rule Name	Name of the rule which generates the log. This rule is configured on the SRX Series or vSRX device.
Profile Name	Name of the profile which filters the traffic that triggered the event.
Client Host Name	Hostname of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Malware info	Information about the malware causing the event.

RELATED DOCUMENTATION

About the All Security Events Page 823
About the Firewall Events Page 828
About the Web Filtering Events Page 831
About the IPsec VPNs Events Page 834
About the Content Filtering Events Page 836
About the Antispam Events Page 838
About the Antivirus Events Page 840
About the IPS Events Page 843

About the Traffic Logs Page

To access this page, click **Monitor > Traffic Logs**.

You can use the Traffic Logs page to view the details of the traffic logs that are generated by managed devices. You can view the traffic logs that are generated in the past 24 hours. These traffic logs are used to debug certain events such as, session create, session delete, and session update and so on. You can view the traffic logs for SD-WAN and Next-Generation firewall deployments.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a graphical representation of Traffic logs in a specified time range (Time Range widget).

The x-axis represents the defined time and the y-axis represents number of traffic logs.

Use the slider to decrease or increase the time range within which you want to view the traffic logs. You can also select from pre-defined time ranges such as 5m, 10m, 20m, 30m, 1h, 2h, 4h, 8h, 16h, 24h, or Custom.

If you select Custom, you must specify the dates and times (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) from when and up to when you want the traffic logs displayed.

- View information related to traffic logs; see [Table 284 on page 851](#).
- View similar traffic logs. Select a traffic log and Click **Show exact match** to view similar log.
- Group the traffic logs based on the options available in the **Group by** field. For example, you can group the traffic logs based on destination country, destination IP, and so.
- Show or hide the columns displayed on the page—Click the Show Hide Columns icon at the top right corner of the page and select the columns that you want displayed in the grid.

- View the traffic logs in non tabular format or raw text by clicking the **More > Show raw log** option.
- Create an alert for a specific traffic by clicking the **More > Create Alert** option.
- Create a report for a specific traffic by clicking the **More > Create Report** option.
- Export a traffic log to a comma-separated values (CSV) file by clicking the **More > Export to CSV** option.

[Table 284 on page 851](#) provides information related to traffic logs.

Table 284: Columns on the Traffic Logs Page

Fields	Description
Log Generated Time	View the time when the traffic log was generated.
Log Received Time	View the time when the traffic log was received by CSO.
Site	View the site name when the traffic log was generated.
Event Name	View the event name of the traffic log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Policy Name	View the name of the policy for which the traffic log was generated.
URL	View the accessed URL name that triggered the traffic log.
Event Category	View the event category of the traffic log (For example firewall or apptrack).
User Name	View the user name.
Action	View the action taken for the event: warning, allow, and block.
Host Name	View the hostname in the log.

Table 284: Columns on the Traffic Logs Page (*continued*)

Fields	Description
Service Name	View the name of the Layer 4 service.
Nested Application	View the name of the Layer 7 application.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
NAT Source Port	View the source port of traffic after NAT.
NAT Destination Port	View the destination port of traffic after NAT.
NAT Source Rule Name	View the source NAT rule name.
NAT Destination Rule Name	View the destination NAT rule name.
NAT Source IP	View the source IP address after the IP address translation.
NAT Destination ID	View the destination IP address after the IP address translation.
Traffic Session ID	View the Session ID mapped by site to an event.
Path Name	View the path name of the log.
Logical System Name	View the logical system name.
Rule Name	View the rule name.
Profile Name	View the name of the Web filtering profile that triggered the log.

RELATED DOCUMENTATION

[About the All Security Events Page](#) | 823

Monitoring SD-WAN Events

IN THIS CHAPTER

- [SD-WAN Events Overview | 853](#)
- [About the SD-WAN Events Page | 854](#)

SD-WAN Events Overview

Service-level agreements (SLAs) define the expected class of service (CoS) for all applications and application groups in a site. The network operator needs tools to measure and monitor the performance metrics for all applications to determine the quality of the network and adherence to an assured CoS. To ensure compliance with SLAs, the network operator also needs tools to take remedial action when network performance deteriorates and SLAs are not being met. SD-WAN link-switch events enable the network to switch WAN links to meet the site's SLA requirements when the network-designated WAN link is unable to meet the site's SLA requirements.

Because SLA parameters override the path preference, in dynamic SD-WAN policies, the SD-WAN network chooses the best possible WAN link for traffic management. The WAN link is chosen based on the SLA parameters defined in the SLA profile. If multiple links match the SLA profile, the least loaded link is chosen. When a policy intent is deployed on a site, if the WAN link chosen by the SD-WAN network is unable to meet the SLA requirements in runtime, then the site switches WAN links to meet the SLA requirements. This link switching is called an SD-WAN event. Link switching also takes into account the priority defined in the SLA profile and SLA profiles with higher priority are given precedence while finding alternate WAN links. The ability of a site to switch WAN links ensures that SLA requirements are met and instances of not meeting the SLA requirements are minimized.

In static policies, link switching cannot occur even if the designated WAN link is unable to meet the SLA requirements, because path preference is defined.

RELATED DOCUMENTATION

[About the SD-WAN Events Page | 854](#)

[Traffic Steering Profiles and SD-WAN Policies Overview | 568](#)

About the SD-WAN Events Page

To access this page, click **Monitor > Link Switch Events** in the Customer Portal.

You can use the SD-WAN Events page to view information about SD-WAN events. An SD-WAN event is triggered when the SLA requirements for a site are not met on its network-designated WAN link and the site switches WAN links to meet the SLA requirements.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a graphical representation of SD-WAN events in a specified time range (Time Range widget)
The x-axis represents the defined time and the y-axis represents number of SD-WAN events.
Use the slider to decrease or increase the time range within which you want to view SD-WAN events. You can also select from pre-defined time ranges such as 2h, 4h, 8h, 16h, 24h, or Custom.
If you select Custom, you must specify the dates and times (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) from when and up to when you want the SD-WAN events displayed.
- View the SD-WAN events that occurred and information related to the events; see [Table 285 on page 855](#).
- Show or hide the columns displayed on the page—Click the Show Hide Columns icon at the top right corner of the page and select the columns that you want displayed in the grid.
- Sort and filter SD-WAN events:

NOTE: Sorting and filtering is applicable only to some fields.

- Click a column name to sort the SD-WAN events based on the column name.
- Click the filter icon (funnel) to toggle the filtering. You can enter the filter parameters in one or more fields and press Enter to display the filtered results.
- Search for SD-WAN events using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

[Table 285 on page 855](#) describes the fields on the SD-WAN Events page.

Table 285: Fields on the SD-WAN Events Page

Field	Description
Time Range	<p>View a graphical representation of SD-WAN events against a defined time range. The x-axis represents the defined time and the y-axis represents SD-WAN events.</p> <p>Use the slider to decrease or increase the time range within which you want to view SD-WAN events. You can also choose from pre-defined time ranges such as 2h, 4h, 8h, 16h, 24h, or Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.</p>
SLA Violation Time	Date and time at which the SLA violation occurred.
Link Switch Time	Date and time at which the link was switched.
Site	Name of the site for which the link was switched.
Connected To	Displays the name of the destination spoke or hub site to which the traffic is being sent.
SLA Profile	Name of the SLA-based steering profile associated with the site.
Reason	<p>Indicates the reason for the link switch.</p> <p>Mouse over the reason to view details of the SLA metrics violated.</p>
Apps	Name of the applications for which the SLA violation occurred.
Department	Name of the department for which the SLA violation occurred.
Source Tunnel	Overlay tunnel of the device <i>from</i> which the link switch took place.
Destination Tunnel	Overlay tunnel of the device <i>to</i> which the link switch took place.
Duration (Sec)	<p>Duration (in seconds) for which the SLA requirement for a site was not met before the site switched WAN links.</p> <p>A duration of 0 indicates that the site switched WAN links before it failed to meet the SLA requirements, and the SLA requirements were met immediately on the new WAN link with no loss in meeting SLA requirements.</p>

RELATED DOCUMENTATION

[SD-WAN Events Overview](#) | 853

Monitoring Applications

IN THIS CHAPTER

- [About the SLA Performance of a Single Tenant Page | 856](#)
- [Viewing the SLA Performance of a Site | 859](#)
- [Viewing the SLA Performance of an Application or Application Group | 863](#)
- [Application Visibility Overview | 865](#)
- [About the Application Visibility Page | 866](#)
- [About the User Visibility Page | 869](#)
- [Viewing Application or User Visibility Data for Specific Sites | 872](#)

About the SLA Performance of a Single Tenant Page

To access this page, select **Monitor > Application SLA Performance > *Tenant-Name* SLA Performance** in the Customer Portal.

You can use the *Tenant-Name* SLA Performance page to view performance reports for all sites in a tenant. You can view the SLA performance of all sites that have met and all the sites that have not met the defined SLA target values for the specified time range. You can customize your view and also the time range for which you want to view the SLA performance.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the SLA performance for all sites in the tenant that have met the defined SLA target values, without switching WAN links, for the specified time range.
- View the SLA performance for all sites in the tenant that have met the defined SLA target values, after switching WAN links, for the specified time range.
- View the SLA performance for all sites in a tenant that have not met the defined SLA target values for the specified time range.
- View the SLA performance for all sites in a tenant in grid or card views.

Select card view or grid view at the top right of the page. By default, card view is selected.

- Customize the time range to view the SLA performance for all sites in a tenant.
- View the SLA performance for multiple departments within a single tenant.

Select the specific department for which you want to view the SLA performance from the drop-down list at the top right of the page.

Field Descriptions

[Table 286 on page 857](#) describes the fields on the *Tenant-Name* SLA Performance page.

Table 286: Fields on the SLA Performance of a Single Tenant Page

Field	Description
Time range	The time range for which you want to view the SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.
View	The view in which you want to display the SLA performance for all sites in the tenant. You can choose between card and grid views. By default, card view is selected.
Sites Not Meeting SLAs	<p>The sites that did not meet the defined SLA target values in the selected time range.</p> <p>Click each site to view more information about the SLA performance of the applications and application groups in the site. See “Viewing the SLA Performance of a Site” on page 859.</p>
Sites Meeting SLAs With Switch	<p>The sites that switched WAN links to meet the defined SLA target values in the selected time range.</p> <p>Click each site to view more information about the SLA performance of the applications and application groups in the site. See “Viewing the SLA Performance of a Site” on page 859.</p>
Sites Meeting SLAs Without Switch	<p>The sites that met the defined SLA target values in the selected time range without switching WAN links.</p> <p>Click each site to view more information about the SLA performance of the applications and application groups in the site. See “Viewing the SLA Performance of a Site” on page 859.</p>

Table 287 on page 858 describes the fields in the card and grid views.

Table 287: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views

Field	View	Description
Name	Card and Grid	View the name of the site.
SLA not met (Time)	Card and Grid	View the average time (in %) during which all the sites in a tenant did not meet the defined SLA target values.
Profiles	Card	View the time (in %) during which defined SLA target values were not met for each SLA profile. The top two profiles with highest priority and the percentage of time during which SLA target values were not met are listed. The remaining profiles and their combined sum of time (in %) for which SLA target values were not met are listed under Others . The SLA profile priority is indicated inside a circle. You can define priority of the SLA profile when you create an SLA profile. Hover over the profile priority to view the SLA profile name.
Profile SLA Not Met	Grid	
App - Groups	Card and Grid	View the total number of applications and application groups in the site.
Switch Events	Card and Grid	View the number of times the site switched WAN links over the number of designated WAN links. A switch event, also called SD-WAN event, occurs when a site switches WAN links to meet the SLA requirements.
Switch Events Per Profile	Card and Grid	View the number of times the site switched WAN links for each profile. You can view the switch events for the top two SLA profiles in the decreasing order of switch events for each profile.

RELATED DOCUMENTATION

[Viewing the SLA Performance of a Site | 859](#)

[Viewing the SLA Performance of an Application or Application Group | 863](#)

[SD-WAN Events Overview | 853](#)

[Adding SLA-Based Steering Profiles | 591](#)

[Adding Path-Based Steering Profiles | 602](#)

Viewing the SLA Performance of a Site

IN THIS SECTION

- [SLA Not Met by SLA Profiles | 859](#)
- [Applications SLA Performance by Throughput | 860](#)
- [SLA Performance for ALL | 862](#)

You can use the **Monitor > Applications > Tenant_name SLA Performance > Site_name SLA Performance** page in the Customer Portal to view the SLA performance for all applications and application groups in a site. You can view the SLA performance for all applications and application groups in a site for a specified time range and in graph or grid views.

The **Site_name SLA Performance** page is divided into the following sections:

SLA Not Met by SLA Profiles

You can use the **SLA Not Met by SLA Profiles** section on the **Site_name SLA Performance** page to view the SLA profiles for which SLA requirements were not met and the time at which they were not met. The y-axis represents the SLA profiles and the x-axis represents the specified time range. The **SLA Not Met by SLA Profiles** section can be viewed and remains the same in both graph and grid views.

To view a graphical representation of SLA profiles for which SLA target values were not met:

1. Select the time range for which you want to view the SLA profiles for which SLA target values were not met. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.

The graphical representation of SLA profiles for which SLA target values were not met is displayed for the selected time range.

2. (Optional) You can use the sliders at the sides of the graph to further customize the time range.

The graphical representation of SLA profiles for which SLA target values were not met is refreshed and displayed for the customized time range. The graphical representation of SLA performance data in the subsequent sections on the page is also refreshed and displayed for the customized time range.

Applications SLA Performance by Throughput

You can use the **Applications SLA Performance by Throughput** section on the **Site_name SLA Performance** page to view average throughput performance of all applications and application groups in a site. You can also customize your view by selecting graph or grid views. In the graph view, you can further select scatter plot or tree map.

To view a graphical representation of average throughput performance of all applications and application groups in a site:

1. Select **Graph View** at the top right of the page. By default, Graph View is selected.

A graphical representation of average throughput performance of all applications and application groups in a site against the target throughput is displayed in the **Scatter Plot** view. The y-axis represents the average throughput. 0% on the x-axis represents the target throughput (in %) defined in the SLA profiles, while the regions on the left and right of the target represent percentages below and above the target throughput, respectively.

A carousel at the bottom of the section also displays the list of all applications and application groups with their SLA profiles, target throughput, and average throughput values.

2. Click **Legend** at the bottom right of the section to view the plotting legend.

The items described in the **Legend** are:

- A single application is represented by a blue circle.
- An application group is represented by a blue square.
- An application or application group whose target throughput value in the SLA profile was modified during runtime is represented by an uncolored circle and uncolored square, respectively.
- The SLA profiles are represented by their priority numbers within the colored or uncolored circles and squares.

3. (Optional) You can use the sliders at the sides of the graph further to customize the time range.

The carousel is refreshed for the customized time range.

4. Click the circles or squares to view more information about the application or application groups. See [“Viewing the SLA Performance of an Application or Application Group” on page 863](#).
5. Select **Tree Map** at the top right of the section to view a list of all applications and application groups in a site and their average throughput values.

A list of all applications and application groups in a site along with their associated SLA profiles and the average throughput values is displayed.

To view a tabular representation of average throughput performance of all applications and application groups in a site:

1. Select **Grid View** at the top right of the page.

A list of all applications and application groups along with their SLA profiles, average throughput, and target throughput values is displayed in a tabular format.

[Table 288 on page 861](#) describes the fields on the Applications SLA Performance by Throughput grid view.

Table 288: Fields on the Applications SLA Performance by Throughput Grid View

Field	Description
Name	View name of the application or application group.
SLA Profile	View the SLA profile associated with the application or application group.
Type	View the type—application or application group
Category	View the category of the application or application group. The value of Category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, Video, and so on.
Sessions	View number of sessions consumed by the application or application group.
Throughput Avg. Performance	View the average throughput performance value (in %) of the application or application group. The upward triangle on the left of the average throughput performance value indicates that the average throughput is higher than the target throughput configured in the SLA profile of the application or application group. The value (in %) denotes the percentage above the target throughput value. Similarly, the downward triangle on the left of the average throughput performance value indicates that the average throughput is lower than the target throughput configured in the SLA profile of the application or application group. The value (in %) denotes the percentage below the target throughput value.

2. (Optional) Click the details icon to the left of the application or application group name to view more information about the application or application group. See [“Viewing the SLA Performance of an Application or Application Group” on page 863](#).

SLA Performance for ALL

View a graphical representation of the performance of the SLA parameters such as round-trip time (RTT), latency, packet loss, and jitter for the specified time range for MPLS and Internet WAN links for all SLA profiles. The y-axis represents the SLA parameters and the x-axis represents the specified time range. You can also view the respective target SLA parameters in the graphs.

NOTE: The graphical representation of the performance of all SLA parameters for the WAN links is available only in the graph view.

To view a graphical representation of the performance of all SLA parameters for the WAN links:

- Select **All** at the top right of the section. By default, All is selected.

A graphical representation of the performance of the SLA parameters such as RTT, latency, packet loss, and jitter for the specified time range for all WAN links is displayed.

- Select **wan_0**, **wan_1**, and so on at the top right of the section to view the performance of the SLA parameters for the MPLS and Internet WAN links. You can enable and configure **wan_0**, **wan_1**, and so on and map them to MPLS or Internet links when you create a site.

The graphical representation of the performance of the SLA parameters such as RTT, latency, packet loss, and jitter for the specified time range is refreshed and only the performance for the selected WAN link is displayed.

- (Optional) Click **Legend** at the bottom right of the section to view the plotting legend for the horizontal dotted lines parallel to the x-axis in the graphs. The horizontal dotted lines represent the respective target SLA parameters of the SLA profiles.

RELATED DOCUMENTATION

[About the SLA Performance of a Single Tenant Page | 856](#)

[Viewing the SLA Performance of an Application or Application Group | 863](#)

Viewing the SLA Performance of an Application or Application Group

You can use the **Monitor > Applications > Tenant-Name SLA Performance > Site-Name SLA Performance** page in the Customer Portal to view the SLA performance for individual applications and application groups in a site. You can also view the SLA performance of the associated SLA profile for all SLA parameters.

To view SLA performance of an application or application groups:

- Click one of the circles or squares in the **Applications SLA Performance by Throughput** section on the **Site-Name SLA Performance** page.

The page that appears displays SLA performance details of the application or application group.

[Table 289 on page 863](#) describes the fields on the application or application group SLA Performance details page.

Table 289: Fields on the Application or Application Group Details Page

Field	Description
Category and Description	View the category of the application or application group. The category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, Video, and so on. You can also view a description of the application or application group.
SLA	View the name of the SLA profile associated with the application or application group.
Target	View the current target throughput defined in the SLA profile associated with the application or application group. If the target throughput was modified during runtime, the date and time when the throughput was modified and the previously defined throughput value are also displayed.
Avg. Performance	View the average throughout performance (in %) above or below the configured target throughput. The average throughput (in Mbps) is displayed within parentheses.
SLA Metrics by Throughput	View a graphical representation of the SLA metrics by throughput during the specified time range for that application or application group. The y-axis represents the throughput (in Mbps). The x-axis represents the specified time range. Hover over the graph to view the throughput value and time at any specified point. You can also view the sessions consumed by the WAN links for the application or application group time range.

Table 289: Fields on the Application or Application Group Details Page (*continued*)

Field	Description
Global SLA Profile Performance	<p>View the performance for all the SLA parameters of the SLA profile associated with the application or application group. The SLA performance is represented by a color-coded donut chart. The section in blue in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were met. The section in red in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were not met.</p> <p>Click the red colored section of the donut chart to view more information about when SLA requirements for the SLA profile were not met. The SLA Profile Performance page appears. The SLA Profile Performance page displays the following fields:</p> <ul style="list-style-type: none"> • SLA Profile—SLA profile associated with the application or application group • Target—Target throughput configured in the SLA profile • SLAs Not Met—Percentage of time SLA requirements were not met for the SLA profile • Sessions—Number of sessions consumed by the application or application group • Start Time—Time at which the WAN links associated with the application or application groups started to fail meeting the SLA requirements • End Time—Time at which SLA profile requirements started to be met again • Avg Val—Average throughput (in Mbps) when the SLA requirements started to fail • Duration—Total duration (in seconds) during which SLA requirements were not met • From—Source WAN link • To—Destination WAN link

RELATED DOCUMENTATION

[About the SLA Performance of a Single Tenant Page | 856](#)

[Viewing the SLA Performance of a Site | 859](#)

Application Visibility Overview

Contrail Service Orchestration (CSO) supports application visibility, a feature that enables you to protect your network against application-level threats.

The feature provides security management information such as the type, bandwidth consumption, and behavior of applications running on your network. As the SP administrator, OpCo administrator, or tenant administrator with the required tenant-level privileges to access the Application Visibility page, you can use this information to identify application-level threats to your network. For example, you can identify threats posed by applications that consume excess bandwidth and cause data loss due to network bandwidth congestion. You can also control the applications at a granular level by managing the type of traffic allowed to enter or exit the network.

You require application visibility because it helps you overcome the various challenges faced by your network. For example:

- Web-based applications use nonstandard ports and encryption, which make effective management of traffic flows challenging.
- Applications such as social networking, peer-to-peer file sharing, and Webmail change their communication ports and protocols dynamically, or tunnel within other commonly used services such as HTTP or HTTPS, to avoid traditional security mechanisms. This makes the implementation of access control challenging.

Benefits of Application Visibility

- Traffic management—Application visibility provides insight into applications running on the network. You can analyze applications running on the network for performance and assurance. In addition, you can define application policies to steer and control applications, on a granular level, to meet Service-level Agreements (SLAs).
- Network threat protection—Use application visibility to identify application-level threats based on the risk level of each application running on the network. You can then mitigate these threats by adding appropriate firewall policy intents to allow, restrict, or block network access to applications.
- Effective bandwidth management—Application visibility provides information about the bandwidth consumption of each application running on the network. You can use this information and rate-limit applications that consume excess bandwidth.

RELATED DOCUMENTATION

[About the Application Visibility Page | 866](#)

[About the User Visibility Page | 869](#)

About the Application Visibility Page

To access this page, select **Monitor > Applications > Visibility**.

There are two ways in which you can view your application visibility data—**Chart View** or **Grid View**. By default, the data is displayed in **Chart View**.

Tasks You Can Perform

You can perform the following tasks from this page:

- View application visibility data in **Chart View**. See [“Chart View” on page 866](#).
- View application visibility data in **Grid View**. See [“Grid View” on page 867](#).
- Select a device to which the application visibility settings are applicable. See [“Viewing Application or User Visibility Data for Specific Sites” on page 872](#).

Chart View

Click the **Chart View** link for a brief summary of the top 50 applications consuming the maximum bandwidth in your network. The data can be presented graphically as a bubble graph, heat map, or a zoomable bubble graph. The data is refreshed automatically based on the selected time range. You can also use the **Custom** button to set a custom time range.

You can hover over your applications to view critical information such as total number of sessions, total number of blocks, category, bandwidth consumed, risk levels, and characteristics. You can also view the top five users accessing your application.

[Table 290 on page 866](#) provides guidelines on using the fields on the **Chart View** of the **Application Visibility** page.

Table 290: Fields on the Chart View

Field	Description
All Devices	Displays application visibility data for all the sites managed by CSO. Click Edit to select individual devices for which you want to view the data.
Show By	Select from the following options to view a user’s data: <ul style="list-style-type: none">• Bandwidth—Shows data based on the amount of bandwidth the application has consumed for a particular time range.• Number of Sessions—Shows data based on the number of sessions consumed by the application.

Table 290: Fields on the Chart View *(continued)*

Field	Description
Time Span	<p>Select the required time range to view a user's data.</p> <p>Use the custom option to choose the time range if you want to view data for more than one day. The time range is from 00:00 through 23:59.</p>
Select graph	<p>Select from the following graphical representations to view an application's data:</p> <ul style="list-style-type: none"> • Bubble Graph • Heat Map • Zoomable Bubble Graph <p>By default, data is shown in the Bubble Graph format.</p>
Group By	<p>Select from the following options to view the application's data:</p> <ul style="list-style-type: none"> • Risk—Grouped by critical, high, unsafe, and so on. • Category—Grouped by categories such as web, infrastructure, and so on.
Number of Sessions	Displays the total number of application sessions.
Number of Blocks	Displays the total number of times the application was blocked.
Bandwidth	Displays the bandwidth usage of the application.
Risk Level	Displays the risk associated with the application. For example, critical, high, unsafe, and so on.
Category	Displays the category of the application. For example, web, infrastructure, and so on.
Characteristics	Displays the characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling, and so on.

Grid View

Click the **Grid View** link to obtain comprehensive details about applications. You can view top users by volume, top applications by volume, top category by volume, top characteristics by volume, and sessions by risk. You can also view the data in a tabular format that includes sortable columns. You can sort the applications in ascending or descending order based on application name, risk level, and so on.

[Table 291 on page 868](#) describes the widgets in this view. Use these widgets to get an overall, high-level view of your applications, users, and the content traversing your network.

[Table 291 on page 868](#) provides guidelines on using the fields on the **Grid View** of the **Application Visibility** page.

Table 291: Widgets on the Grid View

Field	Description
Top Users By Volume	Top users of the application; sorted by bandwidth consumption.
Top Apps By Volume	Top applications using the network traffic, such as Amazon, Facebook, and so on, sorted by bandwidth consumption.
Top Category By Volume	The top category of the application, such as Web, infrastructure, and so on; sorted by bandwidth consumption.
Top Characteristics By Volume	Top behavioral characteristics of the application, such as whether it is highly prone to misuse, the top bandwidth consumer, and so on.
Sessions By Risk	Number of events or sessions received; grouped by risk.

[Table 292 on page 868](#) describes the fields in the table below the widgets. Users are displayed by usernames or IP addresses. When you click a link, the **User Visibility** page appears in a grid view, with the correct filter applied. Sessions are also displayed as links and when you click a link, the **All Events** page appears with all security events.

Table 292: Detailed View of Applications

Field	Description
Application Name	Name of the application, such as Amazon, Facebook, and so on.
Risk Level	Risk associated with the application: critical, high, unsafe, moderate, low, and unknown.
Users	Total number of users accessing the application.
Volume	Bandwidth used by the application.
Total Sessions	Total number of application sessions.
No of Rejects	Total number of sessions blocked.
Category	Category of the application, such as Web, infrastructure, and so on.
Sub Category	Subcategory of the application. For example, social networking, news, and advertisements.
Characteristics	Characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling.

RELATED DOCUMENTATION

[Application Visibility Overview](#) | 865

[Viewing Application or User Visibility Data for Specific Sites](#) | 872

[About the SLA Performance of a Single Tenant Page](#) | 856

About the User Visibility Page

To access this page, select **Monitor > User Visibility**.

Use the User Visibility page to view information about devices (such as top 50 devices accessing high bandwidth-consuming applications and establishing higher number of sessions) on your network. Based on this information, network administrators can choose to rate-limit a device that is accessing applications which consume large bandwidth or create maximum traffic.

Tasks You Can Perform

You can perform the following tasks from this page:

- View user visibility data in **Chart View**. See [“Chart View” on page 869](#).
- View user visibility data in **Grid View**. See [“Grid View” on page 871](#).
- Select one or more sites for which you want to view the user visibility data. See [“Viewing Application or User Visibility Data for Specific Sites” on page 872](#).

Chart View

Click the **Chart View** tab to view the data graphically as a bubble graph, heat map, or a zoomable bubble graph. The data is refreshed automatically based on the selected time span.

You can hover over the chart to view critical information (such as the total number of sessions established and bandwidth consumed) about each user.

Users are represented by the IP address or usernames of their devices on the network.

You can also view the top five applications of each user, based on either their bandwidth consumption or number of sessions established.

[Table 293 on page 870](#) provides guidelines on using the fields on the **Chart View** tab of the **User Visibility** page.

Table 293: Fields on the Chart View

Field	Description
All Sites	<p>By default, the chart displays user visibility data for all the sites managed by CSO.</p> <p>Click Edit to select one or more sites for which you want to view the user visibility data.</p> <p>See “Viewing Application or User Visibility Data for Specific Sites” on page 872 for more information.</p>
Show By	<p>Select the criterion to display information regarding the bandwidth consumed and number of sessions established by applications in the selected time span:</p> <ul style="list-style-type: none"> • Bandwidth—Displays users based on their bandwidth consumption. Users running applications that consume larger bandwidth are represented by larger bubbles or matrices. • Number of Sessions—Displays users based on the number of sessions established. Users running applications that have higher number of sessions established are represented by larger bubbles or matrices.
Time Span	<p>Select the duration (last 15 minutes, last 30 minutes, last 45 minutes, last 1 hour, last 4 hours, last 8 hours, last 12 hours, last 1 day, or custom) for which you want to view the user visibility data.</p> <p>Select Custom to view data for more than one day.</p> <p>The Custom Time page appears.</p> <p>Specify the From date and To date (in MM/DD/YYYY format).The time span is from 00:00 through 23:59.</p>
Select Graph	<p>Select one of the following options to view data graphically:</p> <ul style="list-style-type: none"> • Bubble Graph (default) • Heat Map • Zoomable Bubble Graph

[Table 294 on page 870](#) describes the parameters that are displayed when you hover your cursor over the chart.

Table 294: Parameters on the Chart

Parameter	Description
Number of Sessions	Total number of application sessions established by the user (device).
Bandwidth	Total Bandwidth consumed by the user (device).

Table 294: Parameters on the Chart (*continued*)

Parameter	Description
View All Applications	<p>Click the <i>View All Applications</i> link to view details (such as risk level and category) of all the applications on the network.</p> <p>The Application Visibility page in grid view appears. See “About the Application Visibility Page” on page 866 for more information.</p>

Grid View

Click the **Grid View** tab to view high-level details of the users on your network. You can view widgets that provide information about top users by volume and top applications that create network traffic by volume. The data is also displayed in a tabular format with sortable columns.

[Table 291 on page 868](#) describes the widgets on the **Grid View** of the **User Visibility** page.

Table 295: Widgets on the Grid View

Field	Description
Top Users by Volume	Top users of applications, based on bandwidth consumption, for the selected time span.
Top Apps by Volume	<p>Top applications accessed by users on the network, based on bandwidth consumption, for the selected time span.</p> <p>For example: Amazon</p>

[Table 296 on page 872](#) describes the fields in the table below the widgets.

The table includes sortable columns, with the users (devices) represented by usernames or IP addresses.

Click the Search icon to enter the search text that can include a specific application or user name, or IP address of a device on the network.

The search results are displayed. Click **Clear All** to clear the search results.

Table 296: Detailed View of Users

Field	Description
Applications	<p>Name of the application accessed by a specific user (device).</p> <p>For example: Google</p> <p>NOTE: By default, this column lists only one application per user. If a user accesses more than one application, a +<integer>icon (for example: +2) appears to the right of the application name. The integer indicates the number of additional applications accessed by the user. Click the integer to view all applications accessed by a user.</p>
User Name	IP address or username of the user (device) accessing the applications.
Volume	Bandwidth consumed by a user (who is represented by a user name or IP address).
Total Sessions	Total number of application sessions established by a specific user (device).

Viewing Application or User Visibility Data for Specific Sites

IN THIS SECTION

- [Viewing Application Visibility Data for Specific Sites | 872](#)
- [Viewing User Visibility Data for Specific Sites | 873](#)

You can select one or more sites for which you want to view application visibility or user visibility data (such as bandwidth consumption and number of sessions). By default, the application visibility and user visibility data is displayed for all sites in a tenant.

Viewing Application Visibility Data for Specific Sites

To select the sites for which you want to view the application visibility data:

1. Select **Monitor > Application Visibility**.
The **Application Visibility** page appears.
2. Click the **Edit** link (next to the Show By field).

The **Select Sites** page appears.

3. From the Sites field:

- Click **Selective** to select the sites for which you want to view the application visibility data:

The available sites are displayed in the **Available** column.

- Click **All** to view application visibility data for all sites in the tenant.

If you click All, proceed to step 5.

4. Select the sites from the **Available** column and click the right arrow to move them to the **Selected** column.

5. Click **OK** to save your changes.

You are returned to the Application Visibility page and the application visibility data is displayed for the sites that you selected.

To view application visibility data for other sites, repeat step 2.

Viewing User Visibility Data for Specific Sites

To select the sites for which you want to view the user visibility data:

1. Select **Monitor > User Visibility**.

The **User Visibility** page appears.

2. Click the **Edit** link (next to the Show By field).

The **Select Sites** page appears.

3. From the Sites field:

- Click **Selective** to select the sites for which you want to view the user visibility data.

The available sites are displayed in the **Available** column.

- Click **All** to view user visibility data for all sites in the tenant.

If you click All, proceed to step 5.

4. Select the sites from the **Available** column and click the right arrow to move them to the **Selected** column.

5. Click **OK** to save your changes.

You are returned to the User Visibility page and the user visibility data is displayed for the sites that you selected.

To view user visibility data for other sites, repeat step [2](#).

Monitoring Threats

IN THIS CHAPTER

- [About the Threats Map \(Live\) Page | 875](#)

About the Threats Map (Live) Page

IN THIS SECTION

- [Tasks You Can Perform | 876](#)
- [Field Descriptions | 877](#)
- [Threat Types | 878](#)

To access this page, select **Monitor > Threats Map (Live)** in Customer Portal.

Use this page to visualize incoming and outgoing threats between geographic regions. You can view blocked and allowed threat events based on feeds from intrusion prevention systems (IPS), antivirus, and antispam engines, unsuccessful login attempts, and screen options. You can also click a specific geographical location to view the event count and the top five inbound and outbound IP addresses.

The threat data is displayed starting from 12:00 AM (midnight) up to the current time (in your time zone) on that day and is updated every 30 seconds. The current date and time is displayed at the top right and a legend is displayed at the bottom left of the page.

If a threat occurs when you are viewing the page, an animation shows the country from which the threat originated (source) and the country in which the threat occurred (destination).

NOTE: For threats with unknown geographical IP addresses (private IP addresses), the animation shows the threat originating from the bottom center of the geographical map.

Tasks You Can Perform

You can perform the following tasks from this page:

- Toggle between updating the data and allowing live updates—Click the **Pause** icon to stop the page from updating the threat map data and to stop animations. Click the **Play** icon to update the page data and resume animations.
- Zoom in and out of the page—Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.
- Pan the page—Click and drag the mouse to pan the page.
- View country-specific details:
 - Click a country on the threat map to view threat information specific to that country. A *Country-Name* pop-up appears displaying country-specific information.
 - Click the **View Details** link in the *Country-Name* pop-up to view additional details. The *Country-Name* (Details) panel appears.

For more information, see [Table 297 on page 876](#).

Table 297: Country-Specific Threat Information

Field	Description	Displayed In
<i>Number-of-threat-events</i> Threat Events since 12:00 am	Displays the total number of threat events (inbound and outbound) since midnight for that country. Click the hyperlinked number to go to the All Events page, where you can view more information about the events.	<i>Country-Name</i> pop-up
Inbound (<i>Number-of-threat-events</i>)	Displays the total number of inbound threats for the country and the IP address and the number of events for that IP address for the top five inbound events.	<i>Country-Name</i> pop-up
Outbound (<i>Number-of-threat-events</i>)	Displays the total number of outbound threats for the country and the IP address and the number of events for that IP address for the top five outbound events.	<i>Country-Name</i> pop-up
<i>Number-of-threat-events</i> Events since 12:00 am	Displays the total number of threat events (inbound and outbound) since midnight for that country. Click the hyperlinked number to go to the All Events page, where you can view more information about the events.	<i>Country-Name</i> (Details) panel

Table 297: Country-Specific Threat Information (*continued*)

Field	Description	Displayed In
Number-of Inbound Events	<p>Displays the total number of inbound threats for the country and the number of inbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Device Authentication • Screen <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS Events page.</p> <p>Click the Top 5 IP Addresses (Inbound) to view the IP address and the number of events for that IP address for the top five inbound events.</p>	<i>Country-Name</i> (Details) panel
Number-of Outbound Events	<p>Displays the total number of outbound threats for the country and the number of outbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Device Authentication • Screen <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for screens takes you to the Screen Events page.</p> <p>Click the Top 5 IP Addresses (Outbound) to view the IP address and the number of events for that IP address for the top five outbound events.</p>	<i>Country-Name</i> (Details) panel

Field Descriptions

Table 298 on page 878 displays the fields the Threats Map (Live) page.

Table 298: Fields on the Threats Map (Live) Page

Field	Description
Total Threats Blocked & Allowed	Displays the total number of threats blocked and allowed. Click the hyperlinked number to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events.
Threats Blocked & Allowed	<p>Displays the total number of threats blocked and allowed by the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Device Authentication • Screen <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS Events page (filtered view of the Detail View tab).</p>
Top Target Devices	Displays the top five targeted devices and the number of threats per device. Click the hyperlink for a device to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events for that device.
Top Destination Countries	Displays the top five destination countries and the number of threats per country. Click the hyperlink for a country to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events for that country.
Top Source Countries	<p>Displays the top five source countries and the number of threats per country. Click the hyperlink for a country to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events for that country.</p> <p>NOTE: For threats with unknown geographical IP addresses (private IP addresses), the country name is displayed as <i>Undefined</i>. So, when you click the hyperlinked threat count and go to the All Events page, the filter query uses Undefined as the source country.</p>

Threat Types

The Threats Map (Live) page displays blocked and allowed threat events based on feeds from IPS, antivirus, and antispam engines, unsuccessful login attempts, and screen options. [Table 299 on page 879](#) describes different types of threats blocked and allowed.

Table 299: Types of Threats

Attack	Description
IPS threat events	<p>Intrusion detection and prevention (IDP) attacks detected by the IDP module.</p> <p>The information reported about the attack (displayed on the IPS Events page) includes information about:</p> <ul style="list-style-type: none"> • Source of attack • Destination of attack • Type of attack • Session information • Severity • Policy information that permitted the traffic. • Action: traffic permitted or dropped.
Virus events	<p>Virus attacks detected by the antivirus engine.</p> <p>The information reported about the attack (displayed on the Antivirus Events page) includes information about:</p> <ul style="list-style-type: none"> • Source of the infected file • Destination • Filename • URL used for accessing the file
Spam events	<p>E-mail spam that is detected based on the blocklist spam e-mails.</p> <p>The information reported about the attack (displayed on the Antispam Events page) includes information about:</p> <ul style="list-style-type: none"> • Source • Action: E-mail is rejected or allowed. • Reason for identifying as e-mail spam.
Device authentications	<p>The firewall authentication messages generated due to unauthorized attempts to access the network. The reported information (displayed on the All Events page) contains the reason for authentication failure and the source of the request.</p>

Table 299: Types of Threats (continued)

Attack	Description
Screen events	<p>Events that are detected based on screen options.</p> <p>The information reported about the attack (displayed on the Screen Events page) includes information about:</p> <ul style="list-style-type: none">• Internet Control Message Protocol (ICMP) screening• IP screening• TCP screening• UDP screening

RELATED DOCUMENTATION

[About the All Security Events Page](#) | 823

8

PART

Managing Reports

[Security Reports](#) | **882**

[SD-WAN Reports](#) | **906**

Security Reports

IN THIS CHAPTER

- [Reports Overview | 882](#)
- [About the Security Report Definitions Page | 883](#)
- [Scheduling, Generating, Previewing, and Sharing Security Reports | 886](#)
- [About the Security Generated Reports Page | 889](#)
- [Creating Log Report Definition | 890](#)
- [Creating Bandwidth Report Definition | 894](#)
- [Creating ANR Report Definition | 896](#)
- [Editing, Deleting, and Cloning Log Report Definitions | 899](#)
- [Editing, Deleting, and Cloning Bandwidth Report Definitions | 901](#)
- [Editing, Deleting, and Cloning ANR Report Definitions | 903](#)

Reports Overview

Reports are generated based on the summary of network activity (such as top web applications or viruses detected) and overall network status. To generate reports, you can use the predefined report definitions as is, or you can create custom report definitions that meet your needs for specific data.

The generated report contains a table of contents (TOC) with links to each section of the report. The designated recipients, whose e-mail addresses are included in the report definition, receive the report in PDF format.

You can generate two categories of reports:

Security reports—Provide information about network activity and network status.

SD-WAN reports—Provide information about SLA performance of all sites or specific sites in a tenant.

The following are the types of security reports:

- **Log Reports**—Enable you to analyze event history based on the data criteria (such as filters, aggregation criteria, time span, etc.) that you select.

- **Bandwidth Reports**—Enable you to analyze the bandwidth usage of an application or a user.
- **ANR Reports**—Enable you to analyze business risks in the network, based on application usage and resource usage.

The following are the types of SD-WAN reports:

- **SD-WAN Tenant Performance Reports**—Enable you to analyze tenant performance based on the parameters (top applications by bandwidth, top sites not meeting the SLA, top sites meeting the SLA with switching, sites meeting the SLA without switching, top sites by highest packet loss, and top sites by highest latency, top sites by highest jitter, and current active tunnels) that measure the SLA performance across all sites in a tenant.
- **SD-WAN Site Performance Reports**—Enable you to analyze site performance based on the parameters (top 10 applications and link utilization, top profiles not meeting the SLA, top SLA profiles switching links, top applications by highest packet loss, top applications by highest latency, top applications by highest jitter, SLA performance between two sites, and tunnels created and deleted) that measure the SLA performance of specific sites in a tenant. You can select a maximum of five sites for which you want to generate the report.

RELATED DOCUMENTATION

[About the Security Report Definitions Page | 883](#)

[About the SD-WAN Report Definitions Page | 906](#)

About the Security Report Definitions Page

To access this page, click **Customer Portal > Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

The Security Report Definitions page displays a list of predefined and custom report definitions. To generate reports, you can use the predefined report definitions as is, or you can create custom report definitions.

NOTE: From CSO Release 4.1.0 onward, an Application and Network Risk (ANR) report is the only predefined report definition available on the Security Report Definitions page.

The ANR report provides information about data usage and network risks. The information is consolidated from various predefined report definitions available in the release prior to CSO Release 4.1.0.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a report definition:
 - To create a log report definition, see [“Creating Log Report Definition” on page 890](#).
 - To create a bandwidth report definition, see [“Creating Bandwidth Report Definition” on page 894](#).
 - To create an application and network risk report definition, see [“Creating ANR Report Definition” on page 896](#)
- Edit, delete, or clone report definitions:
 - To edit, delete, or clone a log report definition, see [“Editing, Deleting, and Cloning Log Report Definitions” on page 899](#).
 - To edit, delete, or clone a bandwidth report definition, see [“Editing, Deleting, and Cloning Bandwidth Report Definitions” on page 901](#).
 - To edit, delete, or clone an application and network risk report definition, see [“Editing, Deleting, and Cloning ANR Report Definitions” on page 903](#).
- To schedule, generate reports, preview reports as PDF, and send the reports through e-mail, see [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 886](#).
- To view all the parameters of a report definition, right click the report definition that you want to see the detailed view for and select **Detailed View**, or select the report definition and click **More > Detailed View**. Alternatively, hover over the report definition name and click the Detailed View icon that appears before it.

The Report Definition Details page appears, displaying the same values that you specified for each parameter in the selected report definition.

- To search for a report definition from the list of available report definitions, click the **Search** icon in the top right corner of the page.

Enter the name of the report definition in the search bar and click the Search icon.

The search results are displayed.

Click **Clear All** to clear the search results.

Field Descriptions

[Table 300 on page 885](#) describes the fields on the Security Report Definitions page.

Table 300: Fields on the Security Report Definitions Page

Field	Description
Name	Name of the report definition.
Description	Description of the report definition. For example: Report of data usage by application and network risk.
Type	Type of report definition—ANR, Bandwidth, or Log.
Definition Type	Indicates whether the report definition is predefined (system-generated) or custom (user-created).
Report Content	Details of the sections in the report. For example: Count, Time Duration.
Schedule	Indicates whether the report generation is scheduled at the current time (Now) or for a later date and time (Once).
Recipients	E-mail addresses of recipients to whom the generated report is sent.
Last Generated	Date and time when the report was last generated.
Job ID	Use the job ID to view the status of the task on the Jobs (Monitor > Jobs) page.

RELATED DOCUMENTATION

[Reports Overview | 882](#)
[Creating Log Report Definition | 890](#)
[Creating Bandwidth Report Definition | 894](#)
[Creating ANR Report Definition | 896](#)

Scheduling, Generating, Previewing, and Sharing Security Reports

IN THIS SECTION

- [Editing Report Generation Schedule | 886](#)
- [Generating Reports | 887](#)
- [Previewing Reports in PDF | 888](#)
- [Sharing Reports through E-mail | 888](#)

You can schedule report generation, generate reports, preview reports as PDF, and share the reports through e-mail.

To perform these actions on a report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Select or right-click the report definition on which you want to perform an action and click **More**.

A list of actions that you can perform on the report definition is displayed.

3. Select the appropriate action from the list:

Editing Report Generation Schedule

You can edit the report generation schedule of the selected report definition from the Security Report Definitions page:

1. Select the report definition for which you want to edit the report generation schedule.
2. Click **More > Edit Schedule**. Alternatively, right-click on the selected report definition and select **Edit Schedule**.

The Edit Report Schedule page appears.

3. Specify whether you want to generate the report at the current time or schedule it for a later date and time:
 - **Run now**—Select this option to schedule the report generation at the current time.

- Schedule at a later time—Select this option to schedule the report generation for a later date and time in MM/DD/YYYY and HH:MM:SS formats.

4. Click **OK** to save your changes.

You are returned to the Security Report Definitions page on which a confirmation message, indicating that the report generation schedule is updated successfully, appears.

Generating Reports

You can generate a report at the current time, with either saved settings or custom settings. You can select **Saved Settings** to generate a report based on the values specified in the report definition for the selected report or select **Custom Settings** to modify the values for the Number of Top Logs and the Time Span settings, and generate a report based on the modified values.

NOTE: The modified values are applicable only for the report that is being generated and are not saved in the report definition.

To generate a report:

1. From the Security Report Definitions page, select the report definition based on which you want to generate the report.
2. Click **Run Now** on the Security Report Definitions page. Alternatively, click **More > Run Now** or right-click on the report definition and click **Run Now**.

The Run Report page appears.

3. Do one of the following:
 - Select **Saved Settings** to generate a report based on the values already specified in the report definition.
 - Select **Custom Settings** to modify the values for the Number of Top Logs and Time Span settings, and generate a report based on the modified values.

NOTE: The values that you modify are applicable only for the report that is being generated and are not saved in the report definition.

4. Click **OK** to save your changes.

The Run Report page appears indicating the progress of the report generation. After the report is generated, the **Download PDF Report** link appears on the Run Report page.

5. Click **Download PDF Report**.

Follow your browser instructions to view or save the report in PDF.

Previewing Reports in PDF

You can preview and download the selected report in PDF:

1. Select the report definition based on which you want to generate the PDF of the report.
2. Click **More > Preview as PDF**. Alternatively, right-click on the report definition and select **Preview as PDF**.

The Preview as PDF page appears.

3. Click **Download PDF Report** to view the report in PDF. or click **Cancel** to cancel previewing the report.

The Security Report Definitions page appears.

Sharing Reports through E-mail

You can share the generated report through e-mail:

1. Select the report definition based on which the report is to be generated and shared through e-mail.
2. Click **More > Send Report**. Alternatively, right-click on the report definition and select **Send Report**.

The Edit Recipients page appears:

- **Recipients**—Enter or select one or more e-mail addresses of users to whom you want to send the report.

By default, you can search by first name and select registered users. You can also enter external e-mail addresses.

- **Subject**—Enter the subject line for the e-mail. The maximum length is 2048 characters.
- **Comments**—Enter the text to be included in the body of the e-mail.

The maximum length allowed is 2048 characters.

3. Click **OK** to save your changes.

The Security Report Definitions page appears.

RELATED DOCUMENTATION

| [About the Security Report Definitions Page | 883](#)

About the Security Generated Reports Page

To access this page, click **Customer Portal > Reports > Generated Reports > Security**.

Use this page to view the list of reports that are generated from the Security Report Definitions page. You must click on the report to view the report in PDF.

You can also delete one or more generated reports.

Field Descriptions

[Table 301 on page 889](#) describes the fields on the Generated Reports page.

Table 301: Fields on the Generated Reports Page

Field	Description
Report PDF Name	Type of the report (user created or predefined).
Generated Time	Date and time when the report was generated.
Description	Description of the report.
Definition Name	Name of the report definition.
Generated By	Name of the user who generated the report.
Recipients	Recipients of the generated report.

RELATED DOCUMENTATION

| [Reports Overview | 882](#)

| [About the Security Report Definitions Page | 883](#)

Creating Log Report Definition

Use the Create Log Report Definition page to create log report definitions and generate the corresponding log reports.

Log reports are generated based on the data criteria, which are derived from one or more filters that you select. These reports help you to analyze business risks based on logs from services such as unified threat management (UTM) and firewalls.

To create a log report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Click **Add > Log Report Definitions**.

The Create Log Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 302 on page 890](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to save the log report definition.

The report definition is saved and the Security Report Definitions page appears.

A confirmation message appears on this page, indicating that the log report definition was successfully created.

You can perform various actions on the report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 886](#).

Table 302: Fields on the Create Log Report Definition Page

Field	Description
General	
Report Name	<p>Enter a unique name for the report definition.</p> <p>The name can contain a string of alphanumeric characters and some special characters (colons, periods, dashes, and underscores); no spaces are allowed and the maximum length allowed is 63 characters.</p>

Table 302: Fields on the Create Log Report Definition Page (*continued*)

Field	Description
Description	Enter a description for the report definition; the maximum length (including spaces) allowed is 1024 characters.
Content	
Data Criteria	<p>Click Filters to select one or more filters.</p> <p>The Use Data Criteria From Filter page appears.</p> <p>The list of default and custom filters, which are saved from the Security Events page, is displayed in a tabular format. The table displays the Filter Name, Filter Description, Time Span, and Grouping and Filtering criteria for each filter.</p> <p>Select one or more filters from the list as per your requirement, and click OK.</p> <p>The Create Log Report Definition page appears.</p> <p>When you select one or more filters, new fields appear on the Create Log Report Definition page. The fields are populated with values from the filters. You can either retain the values or change the values if needed. See Table 303 on page 892 for an explanation of the fields.</p>
Schedule	
Schedule Report	<p>Click Add Schedule to schedule the report generation.</p> <p>The Add Report Schedule page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule the report generation at the current time, and click OK. • Schedule at a later time—Select this option to schedule the report generation for a later date and time (in MM/DD/YYYY and HH:MM:SS formats) and click OK. <p>The Create Log Report Definition page appears with details of the report generation schedule.</p>
E-Mail	

Table 302: Fields on the Create Log Report Definition Page (continued)

Field	Description
E-Mail Recipients	<p>Click Add Email Recipients to add e-mail addresses of recipients to whom you want to send the log report.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> Recipients—Enter or select one or more e-mail addresses of users to whom you want to send the report. By default, you can search by first name and select registered users. You can also enter external e-mail addresses (e-mail addresses that are not registered with CSO). Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters. Comment—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters.

Table 303 on page 892 displays the additional fields that appear on the Create Log Report Definition page when you select one or more filters.

Table 303: Additional Fields on the Create Log Report Definition Page

Section	<p>Section number in the log report for a selected filter.</p> <p>Click Delete Section to remove the section and the corresponding filter.</p>
Section Title	<p>Name of the section in the log report.</p> <p>The section title is based on the selected filter.</p>
Section Description	<p>Description for the section in the log report.</p>
Group By	<p>Criteria, such as Nested Application, based on which logs are aggregated.</p> <p>You can select a maximum of two data criteria from the Group By drop-down list.</p>
Time Span (Last)	<p>Duration for which the report is to be generated.</p> <p>The default time span is 3 hours.</p> <p>You can specify the duration in minutes, hours, days, weeks, months, or specify a custom duration.</p>

Table 303: Additional Fields on the Create Log Report Definition Page (*continued*)

	<p>If you select Custom, the Custom Time Range Selection page appears. You must specify the From date and time, and To date and time (in MM/DD/YYYY and HH:MM:SS formats).</p>
Filter By	<p>Filter criteria (such as filtering applications based on http and https protocols) based on which the log report is to be generated.</p> <p>You can use AND, OR, Equal to (=), and Not Equal to (!=) logical operators as values to generate the report.</p> <p>For example: If you want to generate a report with the event category as antivirus and event name as AV_VIRUS_Detected_MT, then the value must be:</p> <p>Event Category = antivirus AND Event Name = AV_VIRUS_DETECTED_MT</p>
Chart	<p>Type of chart to graphically present data on the report.</p> <p>The available options are Bar (default), Comparison Bar, Timeline, Grid, Grouped Grid, Donut, and Bubble chart.</p>
Number of Top Logs	<p>Specify the number of records that you want to retrieve and display for each section in the report.</p> <p>Range: 1 through 20.</p> <p>Default: 10.</p>

RELATED DOCUMENTATION

[About the Security Report Definitions Page | 883](#)
[Creating Bandwidth Report Definition | 894](#)
[Creating ANR Report Definition | 896](#)

Creating Bandwidth Report Definition

You can use the Create Bandwidth Report Definition page to create bandwidth report definitions and generate the corresponding bandwidth reports. Bandwidth reports are used to analyze the bandwidth usage of an application or a user.

To create a bandwidth report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Click **Add > Bandwidth Report Definitions**.

The Create Bandwidth Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 304 on page 894](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to save the bandwidth report definition.

The report definition is saved and the Security Report Definitions page appears.

A confirmation message appears on this page, indicating that the bandwidth report definition was successfully created.

You can perform various actions on the report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 886](#).

Table 304: Fields on the Create Bandwidth Report Definition Page

Field	Description
General	
Report Name	Enter a unique name for the report definition. The name can contain a string of alphanumeric characters and some special characters (colons, periods, dashes, and underscores); no spaces are allowed and the maximum length allowed is 63 characters.
Description	Enter a description for the report definition; the maximum length (including spaces) allowed is 1024 characters.

Table 304: Fields on the Create Bandwidth Report Definition Page (*continued*)

Field	Description
Content	
Number of Top Logs	<p>Specify the number of records that you want to retrieve and display for each section in the report.</p> <p>Range: 1 through 20.</p> <p>Default: 10.</p>
Time Span (Last)	<p>Specify the duration (Custom, last 3 hours, last 6 hours, last 12 hours, or last 24 hours) for which you want the report to be generated.</p> <p>If you select Custom, the Custom Time Range Selection page appears. You must specify the From date and time, and To date and time (in MM/DD/YYYY and HH:MM:SS formats).</p>
Schedule	
Add Schedule	<p>Click Add Schedule to schedule the report generation.</p> <p>The Add Report Schedule page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule the report generation at the current time, and click OK. • Schedule at a later time—Select this option to schedule the report generation for a later date and time (in MM/DD/YYYY and HH:MM:SS formats), and click OK. <p>The Create Bandwidth Report Definition page appears with details of the report generation schedule.</p>
E-Mail	

Table 304: Fields on the Create Bandwidth Report Definition Page (*continued*)

Field	Description
Add E-Mail Recipients	<p>Click Add Email Recipients to add e-mail addresses of recipients to whom you want to send the Bandwidth report.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> • Recipients—Enter or select one or more e-mail addresses of users to whom you want to send the report. By default, you can search by first name and select registered users. You can also enter external e-mail addresses. • Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters. • Comment—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters.

RELATED DOCUMENTATION

[About the Security Report Definitions Page | 883](#)

[Creating Log Report Definition | 890](#)

[Creating ANR Report Definition | 896](#)

Creating ANR Report Definition

You can use the Create ANR Report Definition page to create Application and Network Risk (ANR) report definitions and generate the corresponding ANR reports. ANR reports help you to analyze business risks in a network, based on application usage and resource usage.

To create an ANR report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Click **Add > ANR Report Definition**.

The Create ANR Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 305 on page 897](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to save the ANR report definition.

The report definition is saved and the Security Report Definitions page appears.

A confirmation message appears on this page, indicating that the ANR report definition is successfully created.

You can perform various actions on the report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 886](#).

Table 305: Fields on the Create ANR Report Definition Page

Field	Description
General	
Report Name	Enter a unique name for the report definition. The name can contain a string of alphanumeric characters and some special characters (colons, periods, dashes, and underscores); no spaces are allowed and the maximum length allowed is 63 characters.
Description	Enter a description for the report definition; the maximum length (including spaces) allowed is 1024 characters.
Content	
Number of Top Logs	Specify the number of records that you want to retrieve and display for each section in the report. Range: 1 through 20. Default: 10.
Time Span (Last)	Specify the duration (Custom, last 3 hours, last 6 hours, last 12 hours, or last 24 hours) for which you want the report to be generated. If you select Custom , the Custom Time Range Selection page appears. You must specify the From date and time, and To date and time (in MM/DD/YYYY and HH:MM:SS formats).
Schedule	

Table 305: Fields on the Create ANR Report Definition Page *(continued)*

Field	Description
Schedule Report	<p>Click Add Schedule to schedule the report generation.</p> <p>The Add Report Schedule page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule the report generation at the current time, and click OK. • Schedule at a later time—Select this option to schedule the report generation for a later date and time (in MM/DD/YYYY and HH:MM:SS formats), and click OK. <p>The Create ANR Report Definition page appears with details of the report generation schedule.</p>
E-Mail	
E-Mail Recipients	<p>Click Add Email Recipients to add e-mail addresses of recipients to whom you want to send the ANR report.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> • Recipients—Enter or select one or more e-mail addresses of users to whom you want to send the report. By default, you can search by first name and select registered users. You can also enter external e-mail addresses. • Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters. • Comment—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters.

RELATED DOCUMENTATION

[About the Security Report Definitions Page | 883](#)
[Creating Bandwidth Report Definition | 894](#)
[Creating Log Report Definition | 890](#)

Editing, Deleting, and Cloning Log Report Definitions

IN THIS SECTION

- [Editing the Log Report Definition | 899](#)
- [Deleting Log Report Definitions | 899](#)
- [Cloning Log Report Definitions | 900](#)

You can edit, delete, and clone log report definitions.

Editing the Log Report Definition

You can edit custom log report definitions from the Security Report Definitions page.

To edit a custom log report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Select the log report definition that you want to edit, and click the edit icon (pencil).

The **Edit Log Report Definition** page appears, displaying the same fields that are presented when you create a log report definition.

3. Modify the log report definition fields as needed.

4. Click **OK** to save the changes or click **Cancel** to discard the changes.

The Security Report Definitions page appears.

If you click OK, a confirmation message appears on top of this page.

Deleting Log Report Definitions

You can use the Security Report Definitions page to delete one or more custom log report definitions.

To delete one or more log report definitions:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Select the log report definitions that you want to delete, and click the delete icon. Alternatively, right click on the report definitions that you want to delete and select **Delete Report**.

The **Delete Report Definition** page appears.

3. Click **Yes** to delete the selected log report definitions or click **No** to cancel the deletion.

The Security Report Definitions page appears.

If you click Yes, the selected log report definitions are deleted and a confirmation message appears on top of this page.

Cloning Log Report Definitions

Cloning enables you to create a new log report definition based on an existing one.

NOTE: You can clone predefined and custom log report definitions.

To clone a log report definition:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Right-click the log report definition that you want to clone and select **Clone**. Alternatively, select the log report definition and then select **More > Clone**.

The **Clone log Report Definition** page appears, displaying the same fields that are presented when you create a log report definition.

3. Modify the log Report Definition fields as needed.

4. Click **OK** to save your changes or click **Cancel** to discard the changes.

The Security Report Definitions page appears.

If you click OK, a confirmation message appears on top of this page.

You can perform various actions on the cloned report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 886](#).

RELATED DOCUMENTATION

[Creating Log Report Definition](#) | 890

Editing, Deleting, and Cloning Bandwidth Report Definitions

IN THIS SECTION

- [Editing Bandwidth Report Definitions | 901](#)
- [Deleting Bandwidth Report Definitions | 901](#)
- [Cloning Bandwidth Report Definitions | 902](#)

You can edit, delete, and clone bandwidth report definitions.

Editing Bandwidth Report Definitions

You can edit custom bandwidth report definitions from the Security Report Definitions page.

To edit a custom bandwidth report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Select the bandwidth report definition that you want to edit, and click the edit icon (pencil).

The **Edit Bandwidth Report Definition** page appears, displaying the same fields that are presented when you create a bandwidth report definition.

3. Modify the bandwidth report definition fields as needed.

4. Click **OK** to save the changes or click **Cancel** to discard the changes.

The Security Report Definitions page appears.

If you click OK, a confirmation message appears on top of this page.

Deleting Bandwidth Report Definitions

You can use the Security Report Definitions page to delete one or more custom bandwidth report definitions.

To delete one or more bandwidth report definitions:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Select the bandwidth report definitions that you want to delete, and click the delete icon. Alternatively, right click on the report definitions that you want to delete and select **Delete Report**.

The **Delete Report Definition** page appears.

3. Click **Yes** to delete the selected bandwidth report definitions or click **No** to cancel the deletion.

If you click Yes, the selected log report definitions are deleted and the Security Report Definitions page appears.

A confirmation message appears on top of this page.

Cloning Bandwidth Report Definitions

Cloning enables you to create a new bandwidth report definition based on an existing one.

NOTE: You can clone predefined and custom bandwidth report definitions.

To clone a bandwidth report definition:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Right-click on the bandwidth report definition that you want to clone and select **Clone**. Alternatively, select the bandwidth report definition and then select **More > Clone**.

The **Clone Bandwidth Report Definition** page appears, displaying the same fields that are presented when you create a bandwidth report definition.

3. Modify the bandwidth report definition fields as needed.
4. Click **OK** to save your changes or click **Cancel** to discard the changes.

The Security Report Definitions page appears.

If you click OK, a confirmation message appears on top of this page.

You can perform various actions on the cloned report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 886](#).

RELATED DOCUMENTATION

[About the Security Report Definitions Page | 883](#)

[Creating Bandwidth Report Definition | 894](#)

Editing, Deleting, and Cloning ANR Report Definitions

IN THIS SECTION

- [Editing ANR Report Definitions | 903](#)
- [Deleting ANR Report Definitions | 904](#)
- [Cloning ANR Report Definitions | 904](#)

You can edit, delete, and clone ANR report definitions.

Editing ANR Report Definitions

You can edit custom ANR report definitions from the Security Report Definitions page.

To edit the custom ANR report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Select the ANR report definition that you want to edit, and click the edit icon (pencil).

The **Edit ANR Report Definition** page appears, displaying the same fields that are presented when you create an ANR report definition.

3. Modify the ANR Report Definition fields as needed.

4. Click **OK** to save the changes or click **Cancel** to discard the changes.

The Security Report Definitions page appears.

If you click OK, a confirmation message appears on top of this page.

Deleting ANR Report Definitions

You can use the Security Report Definitions page to delete one or more custom ANR report definitions.

To delete one or more ANR report definitions:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Select the ANR report definitions that you want to delete, and click the delete icon. Alternatively, right click on the report definitions that you want to delete and select **Delete Report**.

The **Delete Report Definition** page appears.

3. Click **Yes** to delete the selected ANR report definitions or click **No** to cancel the deletion.

If you click Yes, the selected ANR report definitions are deleted and the Security Report Definitions page appears.

A confirmation message appears on top of this page.

Cloning ANR Report Definitions

Cloning enables you to create a new ANR report definition based on an existing one.

NOTE: You can clone predefined and custom ANR report definitions.

To clone an ANR report definition:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Right-click on the ANR report definition that you want to clone and select **Clone**. Alternatively, select the ANR report definition and then select **More > Clone**.

The **Clone ANR Report Definition** page appears, displaying the same fields that are presented when you create an ANR report definition..

3. Modify the ANR Report Definition fields as needed.

4. Click **OK** to save your changes or click **Cancel** to discard the changes.

The Security Report Definitions page appears.

If you click OK, a confirmation message appears on top of this page.

You can perform various actions on the cloned report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports”](#) on page 886.

RELATED DOCUMENTATION

[About the Security Report Definitions Page](#) | 883

[Creating ANR Report Definition](#) | 896

SD-WAN Reports

IN THIS CHAPTER

- [About the SD-WAN Report Definitions Page | 906](#)
- [Editing, Deleting, and Cloning SD-WAN Report Definitions | 908](#)
- [Creating SD-WAN Tenant Performance Report Definitions | 910](#)
- [Creating SD-WAN Site Performance Report Definitions | 914](#)
- [About the SD-WAN Generated Reports Page | 917](#)

About the SD-WAN Report Definitions Page

To access this page, click **Customer Portal > Reports > Report Definitions > SD-WAN**.

The **SD-WAN Report Definitions** page appears.

The SD-WAN Report Definitions page displays a list of predefined and custom report definitions. To generate reports, you can use the predefined report definitions as is, or you can create custom report definitions.

NOTE: The SD-WAN Performance Report Definition is the only predefined report definition available on the SD-WAN Report Definitions page.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create SD-WAN tenant performance report definitions. See [“Creating SD-WAN Tenant Performance Report Definitions” on page 910](#)
- Create SD-WAN site performance report definitions. See [“Creating SD-WAN Site Performance Report Definitions” on page 914](#)

- Run a report immediately, edit a schedule, edit e-mail recipients, preview a report in PDF, send reports, and clone reports. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 886](#)
- View details about an SD-WAN report definition—Right-click a report definition and then select **Detailed View** or select the report definition and click **More > Detailed View**. Alternatively, hover over the report definition name and click the Detailed View icon that appears before it.

The Report Definition Details page appears, displaying the same values that you specified for each parameter in the selected report definition.

- To search for a report definition from the list of available report definitions, click the **Search** icon in the top right corner of the page.

Enter the name of the report definition in the search bar and click the search icon.

The search results are displayed.

Click **Clear All** to clear the search results.

Field Descriptions

[Table 306 on page 907](#) describes the fields on the SD-WAN Report Definitions page.

Table 306: Fields on the SD-WAN Report Definitions Page

Field	Description
Name	Name of the SD-WAN report definition.
Description	Description of the SD-WAN report definition.
Type	Type of SD-WAN report definition—Tenant Performance or Site Performance.
Definition Type	Indicates whether the report definition is predefined (system-generated) or custom (user-created).
Schedule	Indicates whether the report generation is scheduled at the current time (Now) or for a later date and time (Once).
Recipients	E-mail addresses of recipients to whom the generated report is sent.
Job ID	Use the job ID to view the status of the task on the Jobs (Monitor > Jobs) page.

RELATED DOCUMENTATION

[Creating SD-WAN Tenant Performance Report Definitions | 910](#)

[Creating SD-WAN Site Performance Report Definitions | 914](#)

Editing, Deleting, and Cloning SD-WAN Report Definitions

IN THIS SECTION

- [Editing the SD-WAN Report Definition | 908](#)
- [Deleting SD-WAN Report Definitions | 908](#)
- [Cloning SD-WAN Report Definitions | 909](#)

You can edit, delete, and clone SD-WAN report definitions from the SD-WAN Report Definitions page.

Editing the SD-WAN Report Definition

You can edit custom SD-WAN report definitions from the SD-WAN Report Definitions page.

To edit an SD-WAN report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Select the SD-WAN report definition that you want to modify, and click the edit icon (pencil).

The Update SD-WAN Performance Report Definition page appears, displaying the same fields that are presented when you create an SD-WAN report definition.

3. Modify the report definition fields as needed.

4. Click **OK** to save the changes or click **Cancel** to discard the changes

The SD-WAN Report Definitions page appears.

If you click OK, a confirmation message appears on top of this page.

Deleting SD-WAN Report Definitions

You can use the SD-WAN Report Definitions page to delete one or more custom SD-WAN report definitions.

To delete one or more SD-WAN report definitions:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Select the SD-WAN report definitions that you want to delete and click the Delete icon. Alternatively, right click the report definitions that you want to delete and select **Delete Report**.

The Confirm Delete page appears.

3. Click **Yes** to delete the selected SD-WAN report definitions or **No** to cancel the deletion.

The SD-WAN report definitions page appears.

If you click Yes, the selected SD-WAN report definitions are deleted and a confirmation message **Successfully deleted report template** appears on top of this page.

Cloning SD-WAN Report Definitions

Cloning enables you to create a new SD-WAN report definition based on an existing one.

NOTE: You can clone predefined and custom SD-WAN report definitions.

To clone an SD-WAN report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Right-click on the SD-WAN report definition that you want to clone and select **Clone**. Alternatively, select the SD-WAN report definition and then select **More > Clone**.

The **Clone SD-WAN Performance Report Definition** page appears, displaying the same fields that are presented when you create an SD-WAN report definition.

3. Modify the SD-WAN Report Definition fields as needed.
4. Click **OK** to save your changes or click **Cancel** to discard the changes.

You are returned to the SD-WAN Report Definitions page.

If you click OK, a confirmation message appears on top of this page.

RELATED DOCUMENTATION

| [About the SD-WAN Report Definitions Page](#) | 906

Creating SD-WAN Tenant Performance Report Definitions

Use the SD-WAN Report Definitions page to create SD-WAN tenant performance report definitions for all sites in a tenant and generate reports based on the definitions. SD-WAN tenant performance reports enable you to analyze tenant performance based on the following parameters that measure the SLA performance across all sites in a tenant:

- Top applications by bandwidth
- Top sites not meeting SLA
- Top sites meeting SLA with switching
- Sites meeting SLA without switching
- Top sites by current active tunnels
- Top sites by highest packet loss
- Top sites by highest latency
- Top sites by highest jitter

NOTE: Only users with the Tenant Administrator role can create SD-WAN tenant performance report definitions.

To create an SD-WAN tenant performance report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Click **Add > Tenant Performance**.

The Add SD-WAN Tenant Performance Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 307 on page 911](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to save the report definition.

The report definition is saved and the SD-WAN Report Definitions page appears.

A confirmation message appears on top of this page, indicating that the report definition is successfully created.

Table 307: Fields on the Create Tenant Performance Report Definition

Field	Description
General	
Report Name	<p>Enter a unique name for the report definition.</p> <p>The name can contain a string of alphanumeric characters and some special characters (colons, periods, dashes, and underscores); no spaces are allowed and the maximum length allowed is 63 characters.</p>
Description	Enter a description for the report definition; maximum length allowed is 1024 characters.
Content	
Time Span	<p>Specify the duration (last 24 hours, last 7 days, last 30 days, or custom) for which you want the report to be generated.</p> <p>If you select Custom, the From and To fields appear:</p> <ul style="list-style-type: none"> • From—Specify the start date and time from which the report should be generated. • To—Specify the end date and time up to which the report should be generated.
Number of Top Logs	Enter the number top of SLA records (1 through 20) that you want to retrieve and display for each section in the report.

Table 307: Fields on the Create Tenant Performance Report Definition (*continued*)

Field	Description
Report Content	<p>Select the content that you want to view in the report.</p> <ul style="list-style-type: none"> • Top Applications By Bandwidth—Displays a report on top applications by bandwidth. • Top Sites Not Meeting SLA—Displays a report on top sites not meeting the SLA performance. • Top Sites Meeting SLA with Switching—Displays a report on top sites meeting SLA performance with link switching. • Sites Meeting SLA without Switching—Displays report on sites meeting SLA performance without switching. • Current Active Tunnels—Displays a report on top 10 sites that have the maximum number of active dynamic mesh tunnels. • Top Sites by Highest Packet Loss—Displays a report on top 10 sites based on the highest cumulative average packet loss across all the links. • Top Sites by Highest Latency—Displays report on top 10 sites based on the highest cumulative average latency across all the links. • Total Sites by Highest Jitter—Displays report on top 10 sites based on the highest cumulative average jitter across all the links. <p>For more information about SLA parameters and dynamic mesh tunnels, see “Traffic Steering Profiles and SD-WAN Policies Overview” on page 568 and “Dynamic Mesh Tunnels Overview” on page 243.</p>
Schedule Report	
Add Schedule	<p>Click Add Schedule to schedule the report generation.</p> <p>The Add Report Schedule page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time.</p> <ul style="list-style-type: none"> • Run now—Select this option to generate the report immediately. • Schedule at a later time— Select this option to generate the report at a later date and time (in MM/DD/YYYY and HH:MM:SS format).
Email Recipients	

Table 307: Fields on the Create Tenant Performance Report Definition (*continued*)

Field	Description
Add Email Recipients	<p>Click Add Email Recipients to add e-mail addresses of recipients to whom you want to send the SD-WAN reports.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> • Recipients—Select e-mail addresses of users to whom you want to send the report. You can select more than one e-mail address. • Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters. • Comment—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters.

RELATED DOCUMENTATION

[Creating SD-WAN Site Performance Report Definitions | 914](#)

[About the SD-WAN Report Definitions Page | 906](#)

[Editing, Deleting, and Cloning SD-WAN Report Definitions | 908](#)

Creating SD-WAN Site Performance Report Definitions

Use the SD-WAN Report Definitions page to create SD-WAN site performance report definitions for specific sites of a tenant and generate the report based on the definitions.

SD-WAN site performance reports enable you to analyze site performance based on the following parameters that measure the SLA performance of specific sites in a tenant:

- Top 10 applications and link utilization for site
- Top profiles not meeting SLA
- Top profiles switching links
- Top applications by highest packet loss
- Top applications by highest latency
- Top applications by highest jitter
- SLA performance between two sites

NOTE: Only users with the Tenant Administrator role can create SD-WAN site performance report definitions.

To create an SD-WAN site performance report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Click **Add > Site Performance**.

The Add SD-WAN Site Performance Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 308 on page 915](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK** to save the report definition.

The report definition is saved and the SD-WAN Report Definition page appears.

A confirmation message appears on top of this page.

Table 308: Fields on the Site Performance Report Definition Page

Field	Description
General	
Report Name	Enter a unique string of alphanumeric characters and some special characters (: . -). No spaces are allowed and the maximum length allowed is 63 characters.
Description	Enter a description for the report definition; maximum length allowed is 1024 characters.
Content	
Time Span	<p>Specify the duration (last 24 hours, last 7 days, last 30 days, or custom) for which you want the report to be generated.</p> <p>If you select Custom, the From and To fields appear:</p> <ul style="list-style-type: none"> • From—Specify the start date and time from which the report should be generated. • To—Specify the end date and time up to which the report should be generated.
Number of Top Logs	Enter the number of top SLA events (1 through 20) that you want to retrieve and display for each section in the report.
Sites	Select one or more sites for which you want to generate the report. You can select up to five sites.

Table 308: Fields on the Site Performance Report Definition Page (*continued*)

Field	Description
Report Content	<p>Select the content that you want to view in the report.</p> <ul style="list-style-type: none"> • Top 10 Applications and Link Utilization—Displays a report on top 10 applications and link utilization for the selected sites. • Top Profiles Not Meeting SLA—Displays a report on top SLA profiles not meeting SLA for the selected sites. • Top Profiles Switching Links—Displays a report on top SLA profiles switching links for the selected sites. • Top Applications by Highest Packet Loss—Displays report on top 10 applications based on the selected site that has the highest average packet loss across SLA profiles. • Top Applications by Highest Latency—Displays report on top 10 applications based on the selected site that has the highest average latency across SLA profiles. • Total Applications by Highest Jitter—Displays report on top 10 applications based on the selected site that has the highest average jitter across SLA profiles. • SLA Performance Between Two Sites—Displays report on top 20 applications based on the performance of SLA parameters (latency, jitter, and packet loss) between the source and destination site that you have selected. <p>For more information about SLA parameters and dynamic mesh tunnels, see “Traffic Steering Profiles and SD-WAN Policies Overview” on page 568 and “Dynamic Mesh Tunnels Overview” on page 243.</p>
Sites	Select one or more sites, from the list of available sites, for which you want to generate the report.
Schedule	
Schedule Report Generation	<p>Click Add Schedule to schedule the report generation.</p> <p>The Add Report Schedule page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule the report generation at the current time, and click OK. • Schedule at a later time—Select this option to schedule the report generation for a later date and time (in MM/DD/YYYY and HH:MM:SS formats), and click OK. <p>The Add SD-WAN Tenant Performance Report Definition page appears with details of the report generation schedule.</p>
E-Mail	

Table 308: Fields on the Site Performance Report Definition Page (*continued*)

Field	Description
E-Mail Recipients	<p>Click Add Email Recipients to add e-mail addresses of recipients to whom you want to send the SD-WAN report.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> • Recipients—Enter or select one or more e-mail addresses of users to whom you want to send the report. By default, you can search by first name and select registered users. You can also enter external e-mail addresses. • Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters. • Comments—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length allowed is 2048 characters.

RELATED DOCUMENTATION

[Creating SD-WAN Tenant Performance Report Definitions | 910](#)

[About the SD-WAN Report Definitions Page | 906](#)

[Editing, Deleting, and Cloning SD-WAN Report Definitions | 908](#)

About the SD-WAN Generated Reports Page

To access this page, click **Customer Portal > Reports > Generated Reports > SD-WAN**.

Use this page to view the list of tenant and site performance reports that are generated from the SD-WAN Report Definitions page.

You must click on the report to view the report in PDF. You can view the generated report for up to 30 days and the report will be deleted after 30 days.

You can also delete one or more generated reports.

Field Descriptions

[Table 309 on page 918](#) describes the fields on the SD-WAN Generated Reports page.

Table 309: Fields on the SD-WAN Generated Reports Page

Field	Description
Name	Name of the SD-WAN report.
Description	Description of the report.
Generated Time	Date and time when the report was generated.
Definition Name	Name of the report definition.
Generated By	Name of the tenant administrator who generated the report.
Recipients	Recipients of the generated report.

RELATED DOCUMENTATION

Reports Overview 882
About the SD-WAN Report Definitions Page 906